Doctoral theses at NTNU, 2023:170

Prosper Kandabongee Yeng

Healthcare Security Practice Analysis, Modelling and Incentivization

Doctoral thesis

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of Philosophiae Doctor
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of Science and Technology

Prosper Kandabongee Yeng

Healthcare Security Practice Analysis, Modelling and Incentivization

Thesis for the Degree of Philosophiae Doctor

Gjøvik, May 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU

Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

ISBN 978-82-326-7044-4 (printed ver.)
ISBN 978-82-326-7043-7 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2023:170

Printed by NTNU Grafisk senter

"The pessimist sees difficulty in every opportunity. The optimist sees opportunity in every difficulty."

(Winston Churchill.)

Declaration of Authorship

I, Prosper Kandabongee Yeng, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

(Prosper Kandabongee Yeng)

Date:

Preface

This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Information Security and Communication Technology at the Norwegian University of Science and Technology, Norway.

The study was carried out during the period from January 2019 to December 2022. The thesis is written on the basis of 15 published research papers and 2 research papers under review. The articles are reformatted to fit the thesis's structure and the contents of the original articles, including the table formats are maintained.

Summary

The human aspect of information security practice has become a global concern. According to Verizon's 2022 data breaches report, over 80% of data breaches were caused by the human aspect, and this trend has been consistent over the past three years. Among the industries, 22% of the violations occurred within healthcare. These breaches are widely caused by external actors (61%) who are motivated by financial gains. Ransomware through phishing attacks has been the preferred tactic. Such incidents have caused financial loss to some hospitals and resulted in the loss of human life.

The security practice in relation to the human aspect is about how people comply with organizational security requirements towards safe-guiding the confidentiality, integrity and availability (CIA) of assets within an IT infrastructure. Technological security configurations have predominantly been relied on as the default and traditional information security controls. Through consistent development, the technological aspect has comparatively been enhanced and matured, thereby, increasing the puzzle for cyber-criminal to circumvent. As a result, cyber-criminals tend to exploit the human aspect as an easy entry point.

This research work, therefore, delves into the human aspect of security practice aimed to contribute towards the fortification of "the human firewall", through incentivising the security practice of healthcare staff. Some research activities have been conducted in this area. However, initial state-of-the-art studies revealed in-comprehensiveness in the existing efforts. As a result, comprehensive approaches were first explored for modelling and analyzing the security practice of healthcare staff in the aspects of data-driven and artificial intelligence or machine learning approaches, attack and defence simulations and psychological, social, cultural and work factors. Furthermore, motivational methods for incentivizing security practices were also explored. This is deemed to be a holistic approach towards enhancing security practices among healthcare staff.

Within the area of data-driven, various methods, including, K-means clustering with iterative and discriminate clustering, were used to assess the security practice in electronic health records (EHR) logs in this research work. Through the assessment, an unusual session duration was revealed in which an average session of about 12,330 hours was detected. Meanwhile, at maximum, a healthcare staff session is estimated to be about 24 hours. Essentially, the K-Means iterative and discriminate (KID) model predicted

normal security practices that could be explored towards the adoption of supervised machine learning methods for real-time abnormal detection and prevention of data breaches.

Furthermore, in this project, the security practices of healthcare staff were assessed through SMS-based phishing simulation attacks. These attacks were performed having analysed and modelled scenarios through literature review work and observational measures. Through state-of-the-art studies, the in-the-wild-field study was adopted to perform a simulated SMS-based attack in a typical hospital. From a total of 167 participants (comprising nurses, doctors and other healthcare staff), about 101 (61%) were victims of the attack. This trend of high victims in a phishing attack was also identified in a related study in this work where out of 830 healthcare staff who were involved in a simulated email-based study, over 50% of the participant fell victim to the attack. Meanwhile, a cybercriminal might need just one person to click the malicious link in a real attack. The higher susceptibility among healthcare staff to the phishing attack, therefore, poses a higher phishing security behaviour risk within the healthcare sector.

Additionally, comprehensive psychological, social, cultural, personal and work-related factors were identified, assessed and analyzed through in-depth literature reviews. Constructs from theories such as the health belief model (HBM), protection motivation theory (PMT), Theory of planned behaviour (TPB), General deterrence theory (GDT) and The big five (TBF) personality theory were adopted and assessed. Through that, variables such as agreeableness were assessed to be a significant positive predictor of self-efficacy (SE) risk and perceived severity (PS) risks.

Following this revelation of varying security practice gaps, originating from multifaceted factors in the assessments, cognitive dissonance (CD) theory, together with other motivational methods, were identified and examined in a controlled experiment. So the CD was used as an independent variable while the other variables were the dependent variables in this controlled experiment. The findings in the experiment showed less susceptibility risk of the actual phishing clicks behaviour among the healthcare staff in the experiment group. To this end, inducing motivational factors such as cognitive dissonance, cues-to-action, and perceived severity, factors among healthcare staff could reverse this global security incident trend in the human aspect.

Future research could explore the adoption of psycho-education with the aid of state-of-the-art training techniques such as virtual reality, and augmented or mixed realities to inculcate long-lasting conscious care behaviour among healthcare staff.

Acknowledgments

"When eating fruit, remember the one who planted the tree"

VIETNAMESE PROVERB

I would like to express my sincere gratitude to my principal supervisor Associate Professor Bian Yang, for his commitment, guidance, support, and advice throughout the entire journey of this research and writing of the thesis. He also permitted me to explore additional research areas of my interest and in various collaborations which have enabled me to establish my personal relationship within the academic community. In his humility, ways of assessment and dedication, my supervisor has become my mentor. My appreciation also extends to Professor Einar Arthur Snekkenes, my co-supervisor for his pieces of advice in the course of this journey.

Additionally, I have been very blessed to have great support during my PhD work. I, therefore, want to use this opportunity to extend my profound appreciation to Egil Utheim, Geir Kristian Lund, Roar Halvorsen and Christian Jacobsen, who facilitated my data collection in healthcare during my PhD work. Furthermore, I wish to extend my gratitude to my wonderful office mates and the academic and administrative staff of the Department of Information Security and Communication Technology, and the entire Norwegian society. Often times the journey path was sometimes slippery, but their warm support system helped me to reach this far. Therefore, I remain extremely grateful.

"Behind every successful man, there is a strong woman". So, I remain very grateful to my wife, Portia Ereng-muo who encouraged me during my low moments in this PhD journey and cushioned me with peace of mind. My deepest gratitude also goes to my children, my entire lovely family and my friends for supporting me throughout this journey.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

"...Information security is a people problem, a managerial problem that does have **SOME** technical solutions..."

WHITMAN ET AL.

1.1 Motivation and problem description

A few years ago, about three million healthcare records were compromised in Norway [32]. This represented an average of half of the total Norwegian population. An insider was believed to have been involved in causing the incident. The citizens humbly asked if the hospital authorities were providing adequate protection for their sensitive data. In another instance, a hacker attacked the IT systems of a major hospital in 2020 in Duesseldorf, Germany [2]. This was a ransomware attack which involved compromising one of the user's terminals. This caused the failure of the IT systems. So scheduled operations were cancelled while emergency cases were transferred to other hospitals. However, a woman was arguably reported to have lost her life due to a one-hour delay in treatment caused by the ransomware attack. Aside from these incidents, the staff of the UK'S national health insurance (NHS) experienced massive phishing attacks [29]. It was reported that 3996 employees of the NHS received 357 million emails, and each staff was targeted with about 89,353 phishing emails.

All these issues relate to the human aspect of security practice [72]. The human aspect of security practice refers to the level of conscious care behaviour of users, in complying with security measures in relation to the confidentiality, integrity and availability (CIA) of assets of an IT infrastructure [94, 28]. The users in the healthcare sector include the healthcare staff such as doctors, nurses, pharmacies, and laboratory personnel, who access patients' records for therapeutic functions [91]. The conscious care behaviour of the healthcare staff in terms of their security compliance level can have varying degrees of security risks.

In recent years, the human aspect of security issues was reported to have contributed to over 80% in global data breaches [69, 70]. Additionally, phish-

ing attacks have also been reported to have sky-rocketed to about 600% to 9000% within the COVID-19 pandemic period [58, 68]. Traditionally, technical security controls have often been adopted in safeguarding the confidentiality, integrity and availability (CIA) of systems as they provide practical and verifiable controls that mitigate the effects of specified threats however, the approach alone has not been an adequate security measure [57]. For instance, the UK and the USA reported a relatively high increase in data breaches that stemmed from the human aspect of security behaviour, after they had a massive implementation of technical security controls. This indicates that relying on technical solutions alone may not be an efficient security measure.

Over-reliance on security controls is synonymous with the famous "Great China Wall". As far back as 200 BC, the problem of human threats to security was eminent [39, 24, 44]. At that time, the Chinese army built a thick tall wall, that was deep into the ground, to protect them against their adversaries. After the Kharn army failed to break through, climb over or dug under the wall, the gatekeeper was bribed. That led to their ingress and their three-times invasion of China. This solidifies the statement that "...Information security is a people problem, a managerial problem that does have some technical solutions... Whitman et al" [73].

So technological configurations including DMZ, firewalls, intrusion detection and prevention systems have over the years improved but less attention has been paid to "the human firewall" [73]. The evidence of this in-balance is the huge proportion of data breaches and a number of attacks on the human aspect of security behaviour.

Moreover, healthcare data is deemed one of the most sensitive and richest data in the world [36]. For instance, financial data might contain both the demographic and payment details of a person. However, Electronic Health Records (EHR) data does contain all these in the financial sector in addition to healthcare-related information [91]. That is why the healthcare data is more attractive and valued at about $ 250 per record compared to a $ 5.40 payment card record [65, 64]. The richness in health data serves as a honey port, attracting the cyber-adversaries.

Data breaches in healthcare affect many stakeholders including the patients, the health facility and the nation. Most countries have the responsibility to protect the privacy of their citizenry. Some of these measures resulted in various regulations such as the general data protection regulation (GDPR) of the EU and the health insurance portability and accountability acts (HIPAA) of the US being enacted [76]. Therefore, in a data breach scenario, that country is seen as irresponsible in the privacy protection of its people. Other adverse effects include dehumanizing patients through the exposure of their health condition to unauthorized persons. Besides, patients' conditions may worsen or even die due to the non-availability of IT

systems for timely therapeutic functions. Health facilities may also suffer from huge financial losses through the data recovery, ransom payments and sanctions from regulatory bodies [78, 76].

Having considered the security repercussions for the healthcare sector, the general objective of this thesis is to assess the security practice of healthcare staff and determine incentive methods that can be used to promote sound cybersecurity practices. The specific objectives, aim and scope of this thesis are presented in section 1.2.

1.2 Research aim, objectives and scope

The aim of this thesis was to provide knowledge in fortifying the human aspect of security practice among healthcare staff, through the assessment and analysis of their security conduct. The research activities that were performed in this thesis are categorized into five (5) major parts as shown in Figure 1.1.

In the first part, the initial review work was conducted to identify the study gaps so as to establish the study direction. In the second part (called the data-driven approach), electronic health records (EHR) logs were analyzed and assessed to determine the security behaviour of healthcare staff in the area of log analysis. In this part of the work, artificial intelligence (AI) methods were first explored and assessed. The appropriate AI methods for analysing security practices were then identified and assessed with simulated EHR logs. The exact purpose was to assess the healthcare security practice status in the logs. Following that, the clustering approach was used to analyze anonymized EHR logs, from a typical hospital, to determine the security practice of its staff.

In the third part (called in this work the attack and defence simulation), a simulation attack was performed on the healthcare staff of the participating hospitals. In these simulated attacks, an SMS-based phishing attack method was adopted. So the security conduct among healthcare staff in the hospitals was therefore assessed and analyzed using the phishing attack method.

In the fourth part, called, the PSC approach, we investigated psychological, social and cultural factors, as well as individual and work factors in relation to healthcare staff security practice. These methods were identified, analyzed and used to assess the security practice of healthcare staff.

In the fifth part, we explored motivational methods that can be used to incentivize security practices. In this task, a control experiment, consisting of three controlled groups and an experiment group, was conducted among healthcare staff in a typical hospital. In this experiment, cognitive dissonance was assessed as the intervention factor in the experiment group.

Essentially, this study in healthcare security practice analysis, modelling and incentivization (HSPAMI) project objectives specifically explored gaps

among the healthcare staff security practice in the area of data-driven, attack and defence and psychological, social and cultural factors as shown in Figure 1.1. Following that, motivation methods were also assessed towards

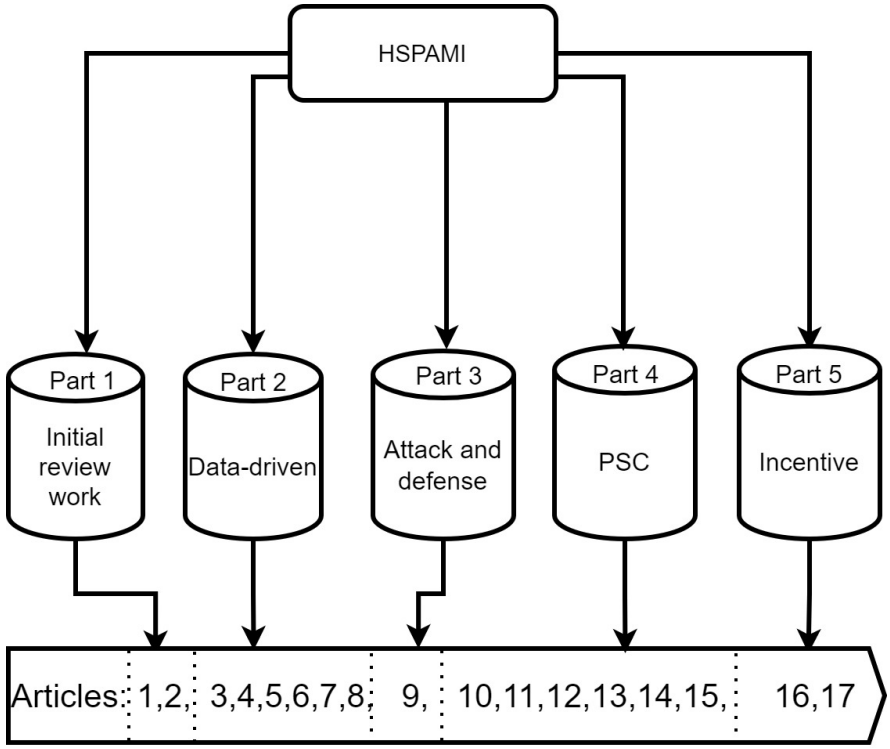


Figure 1.1: HSPAMI study parts.

incentivizing the healthcare staff, aimed at bridging the identified security lapses. The articles and their related mapping to the various parts of the study are shown in Figure 1.1.

1.3 Research questions

Based on the research aim, objective, and motivation, five research questions were formulated to guide this thesis work. The research questions are outlined as follows, and how the articles relate to answering the research questions is shown in Figure 1.2.

Research question 1 (RQ1): How can healthcare staff security practice be modelled and analyzed in the aspect of human factors?

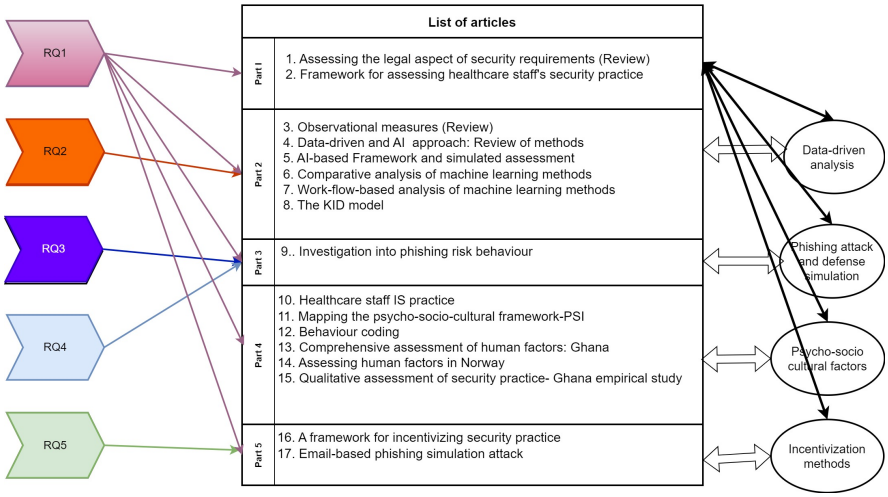


Figure 1.2: Research questions and their mapping to the research contribution.

Psychological, social and cultural theories are commonly used to examine human behaviours. Additionally, the security activities of users can be traced in their generated digital evidence such as logs and browsing history. Moreover, various sources such as security policies, standards, regulations and legal sources, specified required security practices. The purpose of this research question is to therefore explore theories that influence staff security practices, identify the relevant artificial intelligence (AI) methods, attack and defence simulation methods and define a comprehensive security practice that can serve as a yardstick or a baseline for assessing the security behaviour of the healthcare staff.

Research question 2 (RQ2): What is the status of the healthcare staff security practice in the context of psychological, social, cultural and demographic (PSC) context ?

As the healthcare staff operates within the space of a social environment, coupled with individual factors, work factors and psychological factors, this question explored the security compliance level of the staff in this aspect.

Research question 3 (RQ3): What is the status of the healthcare staff security practice in the context of digitization? Typically, healthcare staff security behaviour can be traced in their various digital interactions and accesses within the healthcare IT infrastructure. For instance, the EHR system could have the function of logging all interactions of a healthcare worker if a user accesses a patient record. Patterns of the access behaviour of healthcare staff were explored in this research question and analyzed. AI methods

were explored to access the security practice in electronic healthcare records.

Research question 4 (RQ4): What is the status of the healthcare staff security practice in the area of a phishing attack? Since the healthcare staff are deemed the weakest link [57, 91], they are frequently targeted by cyber adversaries to gain unauthorized access. A phishing attack and defence simulations were conducted to gauge the susceptibility level of healthcare staff in this research question.

Research question 5 (RQ5): How can healthcare staff be motivated to incentivize security practice ? There are different approaches that are often used to improve security practices. So, Various motivational methods were explored to determine their effectiveness towards incentivizing healthcare staff security practices.

1.4 Background

This section presents relevant background and an overview of the thesis to facilitate a better understanding of the remaining aspect of this thesis. Other useful discussions about the study framework, and aspects of the various approaches that were adopted in this work, have also been presented.

1.4.1 An overview and a framework of the HSPAMI project

The research in this thesis is based on the HSPAMI project. It is operated by the Center for Cyber and Information Security (CCIS) of the Norwegian University of Science and Technology (NTNU). The duration of the project is between January 2019 to December 2022, and it is funded by the ministry of health and care of Norway.

Figure 1.3 shows the general framework of the HSPAMI project. The study involves analyzing and assessing healthcare staff security behaviour in different aspects such as phishing attacks, log analysis and psychological, social and cultural aspects. Methods including machine learning, attack and defence simulation and other approaches in the statistical survey were employed. Motivation methods were also explored, modelled and analyzed to determine for suitable ways of incentivising sound security practices. This study provides a framework of a continual process where security gaps are constantly analysed with different approaches and incentive methods are explored towards improvement.

1.4.2 Security practice

According to ISO 27799 standard, the healthcare infrastructure hosts, one of the most sensitive information in the world [36]. Therefore, effective security practice among healthcare staff is an essential complement to the technical solutions to safeguard information assets. Privacy and security practice

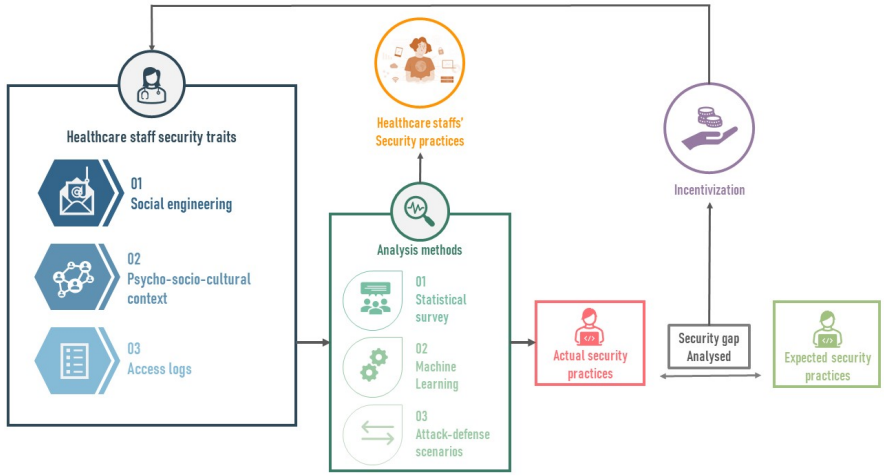


Figure 1.3: HSPAMI study framework.

is the conscious care behaviour required by the healthcare staff (end-users) to observe and comply, by following lay-down rules, regulations and all related security measures while using an IT infrastructure [76]. With recent advances in technology, many end-user-required security actions including patch management and antivirus updates have been automated [30]. However, conscious care behaviour of end users such as appropriate password habits, appropriate use of network and computing resources, effective incident reporting and careful email use that are yet to be addressed by technological measures, are handled in security policies [30]. Effective security practice of healthcare staff has a tendency of mitigating security risk while enhancing the confidentiality, integrity and availability (CIA) of the information assets in the IT infrastructures. The most commonly required areas of security practice for healthcare staff include incident reporting, password management, mobile device use, email use, social media use, incident reporting and information handling [50, 92].

Information security risk management is commonly adopted to identify, assess and manage assets, threats, vulnerabilities and risks within an IT infrastructure [37]. In the HSPAMI project, the possible exploitation of the healthcare staff (being the weakest link) was assessed. The appropriate controls in the form of incentivization were also explored towards mitigation. The ISO/IEC27005:2018, provides a guideline for assessing and managing security risk [37]. The process consists of six activities including context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review, as shown in Figure 1.4.

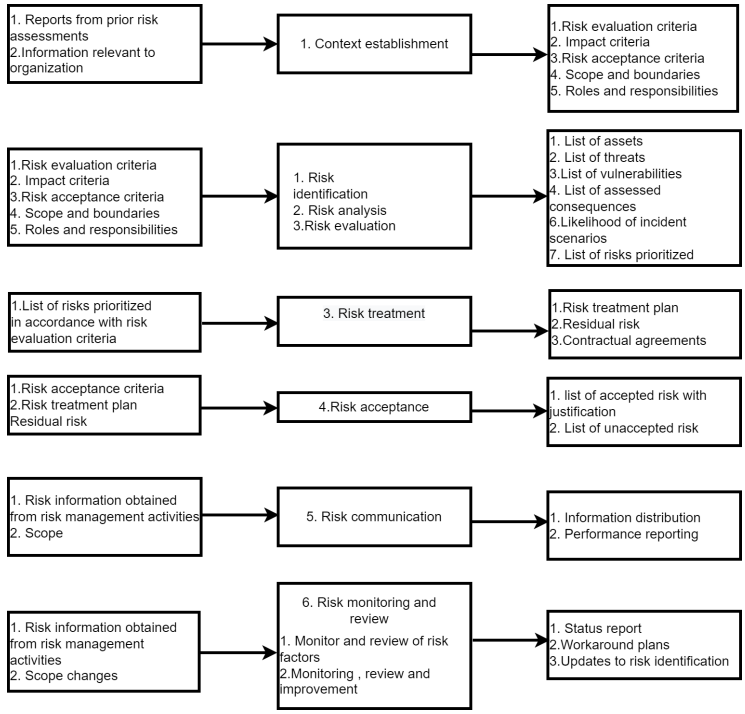


Figure 1.4: Activities or risk management and their input and output based on ISO/IEC 27005.

Each of these activities has a number of inputs and their respective outputs. For instance, in the context establishment, the inputs include reports from prior risk assessment and relevant information as shown in Figure 1.4. In terms of output, risk evaluation, impact criteria, risk acceptance criteria, scope and boundaries, roles and responsibilities are established. Furthermore, risk assessment involves risk identification, risk analysis and risk evaluation. It uses the risk evaluation, impacts and risk acceptance criteria, together with the scope and boundaries as well as the roles and responsibilities of the organization, as input. The output in this activity includes lists of assets, threats, vulnerabilities and controls, and prioritized risk.

Since the aim of the HSPAMI project is to investigate the security practice risks associated with the human aspect, the inputs to context establishment were obtained from previous studies. On the aspect of risk assessment, attack and defence simulation, psychological, social and cultural aspects (PSC) and machine learning in the context of log analysis were adopted. Incentive methods were therefore explored in the area of risk treatment and

risk acceptance. The risks were communicated through discussions in the disseminated scientific papers (as shown in Figure 1.4) while risk monitoring and review were considered in future works.

Moreover, in the aspect of vulnerability principles in ethics, authorities in an organization have the responsibility as moral agents to motivate healthcare staff towards incentivising security practices [87].

1.4.3 Security perceptions

Various theories including the Health Belief Model (HBM), Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB) or Theory of Reasoned Actions (TRA), Social Control (SC) and Technology Acceptance Model (TAM), are some of the psychological, social and cultural theories that have found their way into observing information security practice in the human aspect [86, 34]. For instance, the human aspects such as end users (eg. doctors, nurses and pharmacies), and leadership are normally observed for their security perception, and their belief in the organization's cyber security policy, to predict their likelihood behaviour [47].

In HBM, a person's health-related behaviour is dependent on the belief of the health threats and the efficacy of the recommended actions [16, 47, 47]. This was formulated in the 1950s, to support the prevention drive of sicknesses and to aid the speedy recovery of already sick persons. This model has been used in the healthcare sector to improve health outcomes since people can perceive the severity of the effect of disease or the efficacy of the treatment, to make better health behaviour decisions. The model has the following constructs; perceived susceptibility or vulnerability (PV), perceived severity (PS), perceived benefit(PBf), perceived barriers (PB), cues to action (CA), and self-efficacy (SE). PV is the perceived risk of weakness in contracting a disease or falling victim to a cyber attack. PS is the mindfulness of the adverse impact of the severity of a particular health condition such as death, disability, family life, or social relation. On the aspect of security attacks, PS instances include the implication of loss of data and punishment severity. PB includes the obstacles that are encountered when following the recommended solutions, while the appraisal of one's ability to follow the recommended solutions is known as perceived SE. Additionally, CA is a stimulus that has an effect on a person's decision to follow the recommended solution. There are external or internal stimuli such as pain, disorders, advice, and knowledge of the situation of victims. PBf includes the perception of the opportunities of the recommended course of action that are available. The model has been opined to have some limitations such as its inability to measure attitude, habitual behaviour, and environmental and economic factors.

Ajzen et al proposed TPB which explains the effect of attitude, subjective norms and behavioural control on the behaviour of individuals [7, 59, 42].

Attitude relates to a person's beliefs and feelings based on the direct influence of their knowledge (K) of the IS measures. Both attitude (A) and knowledge constructs can have a direct and indirect influence on the individual's security practice or behaviour [59, 50]. Therefore, the security practice of conscious care behaviour is dependent on the knowledge and attitude of the defined security policies. Healthcare staff's knowledge of the security policies also has a direct effect on their attitude. The knowledge is often acquired through their experience, observations, training, and awareness [4]. The attitude of the healthcare staff towards IS policies refers to their positive or negative intentions towards a specific behaviour. As the knowledge of a particular policy influences attitude, the relative behaviour in that context is expected to be adjusted accordingly. Attitude has explicit and implicit dimensions. In explicit attitude, the individuals are aware of the effect of their behaviour while in implicit attitude, the individuals are unconscious of the effect of their behaviour [8]. Various studies showed significant correlations between these constructs in the context of IS behaviour[66, 49].

In PMT, individuals use threats and coping appraisals for decision-making when they are in stressful or harmful circumstances [45, 35, 91] with the aim of protecting one's self. The threat appraisal has PV and PS constructs which the involved persons usually use to assess their level of threat. PV provides perception measures for assessing the level of susceptibility of the person in a situation, while PS constructs assess the level of severity of the threatening situation. Furthermore, the coping appraisal consists of response efficacy (RE), SE, and response cost (RC). Within the context of PMT, RE is the perception of the effectiveness of the recommended action while RC is the cost component of the recommended measures.

Social control (SC), involves formal and informal social controls [19]. Formal social controls include constructs such as punishment severity, while informal social controls consist of social bonding (SB), peer pressure (PP) and social norms and beliefs.

1.4.4 Personality in relation to security practice

Personality traits are inherent attributes of individual persons that are acquired from biological and environmental factors [27, 3]. This psychological concept has been observed to have a relationship with information security and privacy practice [43]. As personality traits are deemed more stable over a period of time [91, 67, 43, 61], understanding the security practice of the healthcare staff in relation to their personality traits can aid in finding more efficient solutions. There are five most common personality traits as follows [67, 43, 61]:

- Agreeableness trait relates to how well the person gets along with others.

- Conscientiousness determines how careful, deliberate, self-disciplined, and organized an individual is.
- Extroversion is a determinate of a sociable, outgoing, and energetic person.
- Openness measures the extent to which an individual is imaginative and creative
- Neuroticism or Stress Tolerance measures the ways in which individuals react to stress.

1.4.5 Work factors and security practice

In addition to the psychological factors, the work of healthcare staff is characterised by erratic workload [91, 38, 9] and work emergency [86, 90]. Work factors in this study refer to work-related stress, such as workload and work emergencies that are associated with the use of healthcare IT infrastructure. The workload consists of the stress based on the quantum of tasks that one has to perform within a given period, while work emergency refers to the stress in relation to the urgency involve to accomplish a given task [20].

Within healthcare, time is an essential factor where therapeutic measures can be required to be delivered within a given time window without which lives can be lost. All these create work-related stresses, that need to be assessed in the analysis of security practice.

1.4.6 Data driven approach in analysing security practice

Within the healthcare IT infrastructure, individual interactions with the digitized systems can be logged [93]. Such logs include network logs, host-based logs, and specialised applications (such as EHR) logs. The actions of the healthcare staff can be traced and reconstructed to form their unique behavioural profiles. These can therefore be analyzed with various artificial intelligence (AI) or machine learning (ML) methods to determine the security behaviour of the users.

1.4.7 Assessing phishing susceptibility of healthcare staff

There has been a huge surge in phishing attacks in healthcare organisations, however, the scale of susceptibility risk and awareness of the staff largely remains unexamined [53]. Phishing involves deceiving a target through a malicious massage to perform actions that tend to compromise CIA. This study, therefore, examined phishing susceptibility risks among healthcare staff towards providing efficient incentive methods. [25, 58].

1.5 Related work and identified gap

This section presents related frameworks and theories for analysing security practice. The discussion on their limitations and the basis for using the adopted framework are also presented. The related studies were reviewed in relation to the three major parts of the study, thus the PSC approach, data-driven and attack and defence simulation.

Understanding the security practice of healthcare staff cut-across a broad spectrum of human behavioural factors that involves a variety of approaches. For this reason, theories and methods that have been formulated for analyzing human behaviour in various social settings, such as health-seeking, are being adopted into understanding employees' information security behaviour. For instance, Norshima et al developed a conceptual framework for assessing the impact of security awareness and security technology on healthcare cyber staff' security practices [33]. Constructs from Protection Motivation Theory (PMT) and Health Belief Model (HBM) were employed to assess their effect in relation to security awareness and security technology. Similarly, Cannoy et al. also used Technology Acceptance Theory (TAM), Theory of Reasoned Action (TRA), information assurance and security ethical behaviour, organizational culture and health information management [14] in their framework. Both quantitative and qualitative methods were used in these frameworks, in which interviews and questionnaire surveys were conducted. Additionally, Fernandez-Aleman et al., investigated the security practices of healthcare staff in a real clinical setting [23]. Various security governance tools, such as standards, guidelines and recommendations on security and privacy best practices for healthcare staff were identified in a systematic literature review for the development of a survey questionnaire. In the survey, a combined method of both qualitative and quantitative approaches was employed. Safa et al also relied on PMT and the Theory of Planned Behavior(TPB) [59] to ascertain the effectiveness of information security policy awareness on employee security practices. TPB constructs including attitude, subjective norms, and perceived behavioural control, have an influence on the individual way of life [6, 7]. According to Safa et al, experts' opinions were used to develop questionnaire items relating to constructs from the PMT and TPB. All these studies presented frameworks that are useful in the direction of PSC. However, in this digitized era, the adoption of data-driven for assessing security practices cannot be overlooked.

As a result, Boddy et al., conceptually designed a framework and assessed healthcare staff security practice [11] in the area of digitally generated logs. The framework has a processing model for processing input data from computers and medical devices. The framework has a database component for storing and cleaning the data set together with known attack signatures. The entire stored data set was intended for comparison with the

input dataset to detect malicious intentions. The stored dataset was further processed for visualization. The output of the visualization was designed to be interacted by the system users by adjusting parameters to achieve the security situational purpose of the infrastructure. In this experimental study of the framework, the active directory domain controller network statistic (netstat) was captured, analyzed and visualized. In the netstat, the connection type (TCP), source and destination IPs and connection states were captured. In the experiment, a security threat was identified through the most frequent accesses from foreign IP addresses.

In a similar context, Chen et al., created a network anomaly detection sensor (known as SNAD) to determine when specific practices of an insider significantly deviate from a baseline in a collaborative information system [18]. The study was on the premise that if a healthcare staff practice is an anomaly, the similarity of the network of collaborative staff' practices will be higher when the anomalous user is suppressed from the network group. So, a model was developed for each patient's medical record in relation to a group of authenticated healthcare staff who have related access to the subject. A subject-user bipartite graph as a binary matrix was further developed for the similarity measure. The significance of the similarity of the user group with and without the potentially malicious user was determined. SNAD was assessed with access logs of patient records of a large electronic health record system (6,015 users, 130,457 patients and 1,327,500 accesses) and it was comparatively more effective.

Recently, Boddy et al., studied a Local Outlier Factor (LOF)-based data analytic technique, to analyze Electronic Patients Records (EPRs) data and provided context awareness to spot poor security practices [12]. The statistical variables used included Frequency, Mean, Median, Mode, Standard Deviation, Minimum, Maximum, 1st Quartile, 3rd Quartile features, 5th Percentile and 95th Percentile features of the dataset for each User, Patient, Device and Routine. These variables were processed and used to detect outliers through the measurements of local deviations. A LOF anomaly score was determined for each of the User, Patient, Device and Routine IDs. The anomaly score was determined by measuring the local distance of density and determining how far-away the value was in relation to the k-nearest neighbours. A LOF anomaly score of 1 indicated that an object was comparable to its neighbours and represents an in-lier. A value below 1 was considered a dense region, and an in-lier, however, a value with a significant measure greater than 1 was considered an outlier. The algorithm detected 144 outliers in an unlabeled data set of 1,007,727 audit logs which consisted of 0.66% of the users on the system, 0.17% of patient record accesses, 0.74% of routine accesses, 0.53% of the devices used in a specialist Liverpool (U.K.) hospital.

Again, the frameworks that were adopted in [18, 12, 12], shared knowl-

edge of how a data-driven approach can be adopted in assessing the staff's security behavioural pattern, notwithstanding, the data-driven approach cannot be used to investigate into other security conducts. As a result, various frameworks also explored social engineering methods to analyze users' cyber security practices in that direction. According to Wright et al., social engineering is one of the most popular methods that is habitually used by cyber adversaries to manipulate healthcare staff. A large proportion of the victims are most susceptible, in their effort to follow security regulations [74]. Social engineering involves phishing- the act of tricking users to fall victim to adversarial attacks [58]. The practice often involves manipulation and deceiving legitimate system users to click a link or divulge confidential information including, credential information. Some users sometimes take the bait by clicking on malicious links [25, 26], or enter their credentials on the hacker's site [63]. This gives the adversary the opportunity to gain unauthorized access to the system of their victims. The clicking of malicious links may also lead to other forms of attacks such as ransomware attacks, cross-site request forgery and cross-site scripting [46]. In this regard, Gordon et al., conducted a phishing attack simulation to profile victims for training with the aim to improve their abilities against phishing attacks [26]. A phishing email was periodically sent to a large group of healthcare workers. Participants who clicked the link about 5 times before the 16th round of the campaign were tagged as offenders in the study. From a total of 5416 participants in the phishing simulation exercise, over half of the users clicked on at least 2 of the simulated phishing emails and about a quarter of them were profiled as offenders for intervention measures. The victims who were labelled as offended were then informed of their vulnerability nature to phishing attacks. They were subsequently trained on the overview of phishing, phishing scenarios, and how to identify such attacks.

Additionally, a phishing simulation exercise was conducted between 2011 and 2018 across 6 US health institutions because email phishing was identified as a major attack vector [25]. The exercise aimed to describe the practice of phishing simulation and to measure the level of vulnerability of healthcare employees in phishing attacks. A total of 2 971 945 phishing emails were sent in 95 simulated phishing campaigns. The findings showed that 422 062 (14.2%) were susceptible. The rate was that out of every seven emails sent, one of them was often clicked on by healthcare staff. In the study, it was realised that increasing the number of phishing campaigns correlated with decreased click rate. This translates that there is a potential benefit of phishing simulation and awareness. Motivated by the many threats to healthcare data and the IT infrastructure, Rizzoni et al also recently conducted a phishing simulation exercise in a major Italian hospital with over 6000 healthcare staff [58]. In this study, three phishing campaigns were launched within four-months intervals. The goal was to compare staff

susceptibility to general and customized phishing emails. From the study, the staff are more likely to be victims of customized phishing emails as compared to general emails. Because in the initial campaign, 64% of the staff failed to be victims of the general email as compared to 38% of the customized email. Furthermore, a number of related studies, [38, 63, 53, 5], investigated phishing-related conducts of healthcare staff, using the in-the-wild-field approach to appraise the susceptibility level of healthcare staff of the participating organization in order to provide suitable fortifications.

The gist of the related studies shows that while the frameworks of [11, 18, 12], assessed healthcare security practice having adopted the use of digitally generated logs of the healthcare staff, the frameworks developed by [33, 23, 59] were much skewed to only psycho-socio-cultural aspects. Aside from that the studies conducted in [74, 26, 25, 58, 38, 63, 53, 5] obtained information security practice metrics of the healthcare staff through analyzing their phishing attack behaviour. All these studies, therefore, contributed knowledge in assessing healthcare staff security practice, in their various aspects but none of the frameworks adopted a holistic approach to comprehensively examine the healthcare staff security behaviour in the various hospitals [90]. For instance, While security gaps in psychological traits and ethics are essential, studying and covering security gaps in this aspect alone may not be sufficient since such frameworks did not incorporate other aspects (such as data-driven or phishing attacks) in which the healthcare staff' security practice can be traced.

In contrast to these reviewed frameworks and based on these gaps, the HSPAMI framework [90] combined these separated studies into a comprehensive framework as shown in Figure 1.3. Based on the findings, a holistic approach to assessing the healthcare staff's security conduct will result in identifying more comprehensive security gaps where a holistic solution can be defined for effective incentivization. This holistic approach is deemed efficient and a novel contribution to the mitigation efforts in cyber security compliance measures.

1.6 Research method

The traditional scientific research methodology, described in [13, 40] and depicted in Figure 1.5, was adapted in this research work. So, the research problem, of how to assess healthcare staff security practice and how to determine effective incentive methods to mitigate security malpractices, was first defined. Following that related studies were extensively reviewed [90, 91, 85, 86, 92] to define the research questions as specified in section 1.3. This gives us a clear picture of the study structure as shown in Figure 1.6. Subsequently, various research hypotheses, frameworks and models were developed and analyzed in the areas of attack and defence simulation, data-

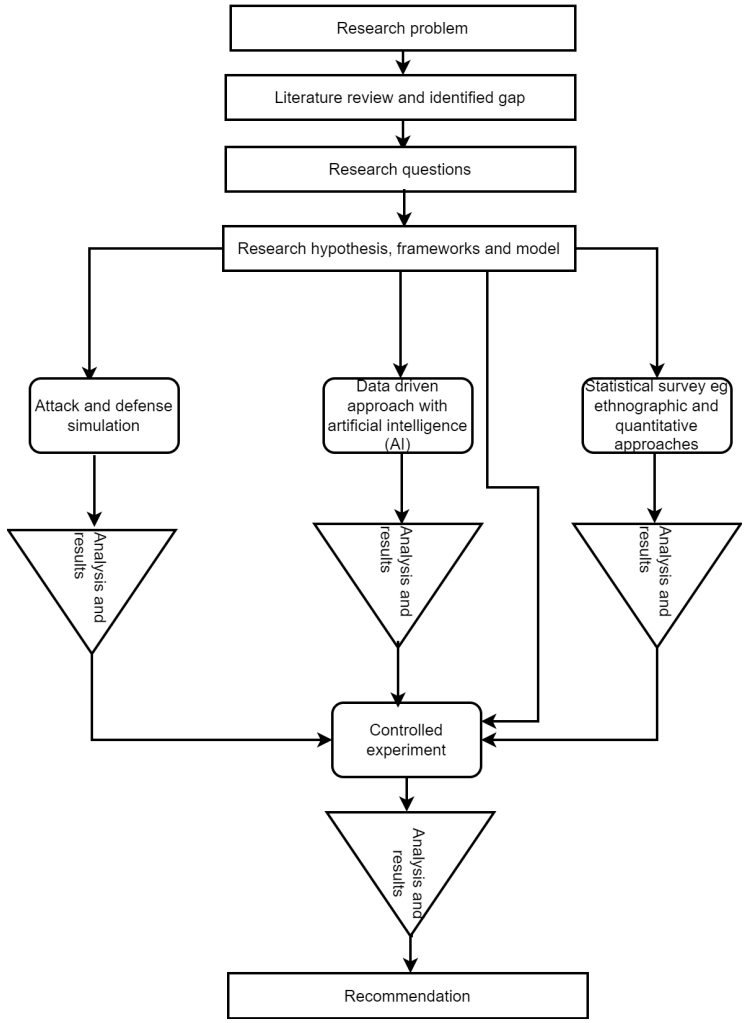


Figure 1.5: Research methodology

driven approach and statistical survey. The results were finally obtained.

The high-level methods that were used in this work are summarized in Figure 1.6. From Figure (1.6), the security practice of healthcare staff in a typical hospital was assessed with a statistical survey and practical analysis.

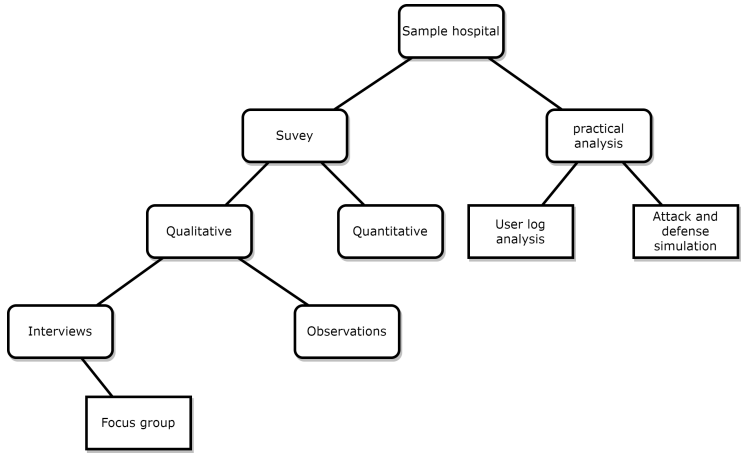


Figure 1.6: Study structure

A highlight of several methods that were used to achieve the study objective in the variant parts of the study is shown in Figure 1.6 and in Table 1.1. Both qualitative and quantitative approaches were employed in the statistical survey in the psychological, social, and cultural aspects of the study. Aside from these methods, the study structure also includes practical analysis in which EHR access logs were analyzed with machine learning methods. Additionally, we simulated phishing attacks on participants to determine their susceptibility levels. A further explanation has been provided in subsection 1.6.1, 1.6.2, 1.6.3 and 1.6.4.

1.6.1 PSC with qualitative and quantitative method

In the assessment of the psychological, social, cultural and work factors (PSC) of the healthcare staff, we conducted in-depth literature reviews [91, 86] in this area. Among others, we explored the various PSC factors that affect healthcare staff security practice and the methods that can be used to analyse these factors. A literature survey was first conducted in [91], where we searched for journal and conference papers relating to behavioural theories and healthcare staff security practice. To obtain the methods that can be used to examine the behaviour of the healthcare staff, only studies that implemented and evaluated these theories were included in the study. Various

Table 1.1: Summary of methods used

	Research area			
Method/Approach	**Data-driven**	**Attack and defense**	**PSC**	**Incentivization analysis**
Machine learning/AI	☑	☐	☐	☐
Quantitative literature survey	☐	☑	☑	☑
Observation in qualitative	☐	☑	☑	☑
Focus-group study	☐	☐	☑	☐
In-the-wild-field-study email-based	☐	☑	☐	☑
In-the-wild-field-study SMS-based	☐	☑	☐	☐
Controlled-experiment	☐	☐	☐	☑
Design science	☐	☑	☐	☐

methods including quantitative surveys, interviews and shadow observing healthcare staff were identified in the study. However, none of the studies adopted a combined approach of these methods to investigate into healthcare staff security practices. A quantitative survey uses a questionnaire to collect and report numerical responses from the study participants. However, human behaviour can not be perfectly assessed with only quantitative methods as people may report their intentions in a quantitative way while their actual behaviour remains in their mind and practice [21]. Therefore, augmenting the quantitative approach with interviews, and observations are better steps to have an effective assessment. The quantitative methods include gathering useful verbal information (through interviews and observations), text or pictures to present a fuller knowledge of the study area. Therefore, adopting the interview and observational approaches in combination with the quantitative methods was considered more effective in this work, in assessing the healthcare staff security practice.

1.6.2 Data driven and machine learning methods

The data-driven approach in information security analysis involves the engagement of data in assessing and mitigating security issues [56]. This approach was traditionally common for bank fraud detection and anomaly-based intrusion detection. The adoption of data-driven, security controls, was not very common due to the complexities associated with running queries in large-scale unstructured data. So most companies used to even delete logged data after a fixed specified time because of lack of storage capacity. But with the advent of AI/Machine learning methods, combined with increased data storage media, a data-driven approach for analysing security behaviour is becoming popular [15].

So, in the area of data-driven, a systematic approach was used to review related work with the aim to identify, analyze and assess various AI methods that can be used to analyze healthcare staff's security conduct in a typical hospital. Between June 2019 and December 2019, we searched in IEEE Explore, Google Scholar, Science Direct/Elsevier, and ACM digital for related peered reviewed journal and conference papers. Kye words such as AI, healthcare, machine learning, anomaly, and intrusion were used. To have a broader and more inclusive method, time-bound was not restricted in the search strategy of these articles. From the identified papers, we further collected and categorized the data to determine the types of AI methods, types of input, application scenarios and performance measures [93]. In this review, we identified various methods including nearness neighbour (KNN), support vector machine (SVM), Random Forest and Decision tree. The challenge is that these methods are supervised-based learning methods and therefore rely on labelled data to classify the security practice of the healthcare staff. So in a situation where there are unlabeled data for training, analyzing the security practice could be a challenge. This guided us to demonstrate how to use unsupervised methods in analysing security practice in EHR in [84].

1.6.3 Attack and defence simulation with statistical survey

Attack and defence simulation among healthcare staff involves the performance of a simulated cyber-attack on users in order to assess their susceptibility level [10, 71, 17]. It involves scenarios where simulated malicious links are embedded in emails or SMS with the aim to trick participants into clicking on the malicious links or sharing confidential information.

So in the area of the practical assessment, phishing-related security conducts of the healthcare staff were also explored. As digital transformation is evolving, the use of mobile devices within the healthcare sector may soon become a norm. With this foresight, simulating the SMS-based attacks, is in good advance direction to mitigate future malware and rootkit infection of healthcare systems through link clicks and ransomware attacks [51].

A thorough literature study was conducted in [55] The research questions that were addressed include the state-of-the-art methods for analyzing phishing security practice in healthcare, attack types, ethical dilemmas in phishing-related studies and phishing attack tools among others. From the findings, statistical survey-based studies, laboratory experiments and in-the-wild-field studies were commonly used to establish the phishing-related security behaviour of the healthcare staff. Among these methods, the in-the-wild-field study is most effective for the following reasons; first, lab-based phishing attack does not present the natural environment of the participants and this tends to influence the outcome of the study. Similarly, a questionnaire-based study involves sending survey questions to partici-

pants to indicate their intended behaviour. This method does not also assess the actual behaviour as participants only report their intended behaviour. As a result of these gaps, a combination of both questionnaire-based and in-the-wild-field studies was adopted. Ethical guidelines to successfully execute SMS based in-the-wild-study were followed as specified in the study [55].

1.6.4 Motivational methods to incentivise security practice

In this aspect of the study, we experimented with cognitive dissonance (CD) to assess how to incentivise security practices among healthcare staff. In digitalized healthcare systems, malicious attackers have the tendency to install malware and rootkits on healthcare systems through malicious link clicks by users, which can lead to ransomware attacks [51]. Therefore method was adopted, having conducted a literature survey into motivational methods for incentivising security practice. From the existing studies, a controlled experimental study and field observational studies were employed in this study. In a controlled experiment, the participants were assigned into groups and the treatment or intervention (CD) was administered to one of the groups, while the other groups were not provided with any intervention [21]. Usually, even if an intervention is provided, that intervention is varied across the groups. In the observational study, participants are surveyed with the aim of observing some factors without varying among the participants. A controlled experiment with two levels (self-reported intended behaviour level and actual behaviour level), thus the control group and the experiment group, was adopted in this work to assess the influence of cognitive dissonance since the controlled-experiment approach is considered to be comparatively suitable for assessing the effect of interventions.

In this study, an email-based phishing simulation called go-phish [1], was set up and pretested using the design science approach (DSM). DSM is predominantly used within the engineering field to efficiently solve real-world problems [31, 52]. The DSM has some analytical techniques that are often used in research functions in information systems [41]. It is used to create and evaluate the effectiveness of IT artefacts, with the object of solving real and identified organizational problems. The artefacts include models, constructs, and frameworks. [52, 41, 31].The DSM require the following processes; identify or explicate the problem, define the requirement, design and develop artefacts, demonstrate artefacts, and evaluate artefacts. In explicating the problem, a real-world problem that is significant in global contexts is assessed and analyzed. In defining the requirement within the DSM framework, an artefact, transforming the problem into demand is created. In the activity of design and development, an artefact that addresses the defined problem and requirement is created. The structure and functionality of this product are also specified. The feasibility of the artefact is further demon-

strated to illustrate how the artefact can solve the specified problem. This is performed within the "demonstrate artefact" activity. Finally, in the evaluation activities, the artefact is assessed to determine the extent to which it can solve the specified problem. Having defined the research problem and requirement through state-of-the-art studies [55, 1], artefacts such as the phishing simulation frameworks were developed and tested with a test group. The test group included hospital staff, two chief technical officers of a healthcare IT provider and two PhD students who were not part of the study participants. This was in fulfilment of the demonstration and evaluation requirement of the design science approach.

1.6.5 Ethical considerations in HSPAMI

In this research work, ethical clearance was first obtained from the Norwegian centre for research data (NSD). Additionally, since, the study was being conducted within healthcare and involved the use of healthcare log data of healthcare staff, ethical consideration was further obtained from the regional committees for medical and health research ethics (REK) of Norway. Furthermore, since the research was extended to Ghana, ethical clearance was obtained from the Kintampo health research centre ethical committee of Ghana. Aside from these, explicit permissions and consent were obtained from the healthcare facilities and individuals who took part in this study.

1.7 Summary of contribution

Various contributions have been made in an effort to answer the specified research questions as outlined in section 1.3. This was achieved by using various theories and methods as shown in Table 1.2, and having followed the research methods in section 1.6. The contribution in this thesis was also based on the motivation of the study as stated in section 1.1, the background of this research work, in section 1.4 and the limitations of related studies as presented in section 1.5. The specific contribution is outlined in this section and depicted in Figure 1.2. The contribution is presented based on the five parts of the study while pinpointing the research questions as shown in Figure 1.2 outlined in section 1.7.1.

1.7.1 List of included research publications

In total, seventeen (17) articles were included in this study from the five parts of the study to answer the five research questions. Six (6) papers were published in Part II (data-driven approach), one paper was published in the attack and defence simulation (part III), and six (6) articles were published in part IV, which relates to psychological, social, cultural and work factors, and

Table 1.2: Theories and methods used

#	Research question	Theory or Method	Category	Reference
1	RQ2	Naive Bayes, k-nearest neighbor,neural network,logistic regression,random forest,decision tree,support vector machine.	Supervised machine learning	[85, 79, 80]
2	RQ2	K-means clustering	Unsupervised machine learning	[84]
3	RQ3	HBM and PMT, TPB	Psychological theory	[83]
4	RQ3	Work emergency and workload	Work factors	[83]
5	RQ4	Behaviour Coding	Psychological theory	[54]
6	RQ4	PMT, TPB, HBM, SC, GDT, TBF, TPB	Psychological, Social	[81, 81]
7	RQ4	Work load, Work emergency	Work factors	[81, 81]
8	RQ4	Organizational culture	Culture	[81, 81]
9	RQ5	PMT, HBM, TBF, TPB	Psychological,	[1]
10	RQ5	PMT, HBM, The Big Five or personality	Psychological	[1]

two (2) papers were published in part V , on incentivising for security practice as shown in Figure 1.2. Additionally, this list includes two published literature-reviewed papers which were published in the initial exploration of this work. They served as a foundation for all four parts of this thesis work and are labelled as part I. The following sections outlined the list of publications in the various parts of the study.

1.7.1.1 List of contributions in the initial review work that concerns all parts of this study (part I)

1. [78] Yeng, P. K., Fauzi, M. A., Sun, L., & Yang, B. (2022). Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development. JMIR Human Factors, 9(2), e30050.

2. [90] Yeng, P. K., Yang, B., & Snekkenes, E. A. (2019, December). Framework for healthcare security practice analysis, modeling and incentivization. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 3242-3251). IEEE.

1.7.1.2 List of contribution in data-driven approach (Part II)

3. [76]Yeng, P., Yang, B., & Snekkenes, E. (2019, July). Observational measures for effective profiling of healthcare staffs' security practices. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 397-404). IEEE.
4. [93]Yeng, P. K., Nweke, L. O., Woldaregay, A. Z., Yang, B., and Snekkenes, E. A. (2020, September). Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. In Proceedings of SAI Intelligent Systems Conference (pp. 1-18). Springer, Cham.
5. [85] Yeng, P. K., Nweke, L. O., Yang, B., Fauzi, M. A., and Snekkenes, E. A. (2021). Artificial Intelligence–Based Framework for Analyzing Health Care Staff Security Practice: Mapping Review and Simulation Study. JMIR Medical Informatics, 9(12), e19250.
6. [79]Yeng, P. K., Fauzi, M. A., and Yang, B. (2020, December). Comparative analysis of machine learning methods for analyzing security practice in electronic health records' logs. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 3856-3866). IEEE.
7. [80]Yeng, P. K., Fauzi, M. A., and Yang, B. (2020, December). Workflow-based anomaly detection using machine learning on electronic health records' logs: A Comparative Study. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 753-760). IEEE.
8. [84] P. K. Yeng, M. A. Fauzi, B. Yang and S. Y. Yayilgan, "Analysing digital evidence towards enhancing healthcare security practice: The KID model," 2022 1st International Conference on AI in Cybersecurity (ICAIC), 2022, pp. 1-9, doi: 10.1109/ICAIC53980.2022.9897055.

1.7.1.3 List of contributions in attack and defence simulation (Part III)

9. [83]Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). Investigation into Phishing Risk Behaviour among Healthcare Staff. Information, 13(8), 392.

1.7.1.4 List of contributions in PSC aspect (Part IV)

10. [91] Yeng, P. K., Yang, B., & Snekkenes, E. A. (2019). Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. pHealth 2019, 239-245.

11. [86]Yeng, P. K., Szekeres, A., Yang, B., & Snekkenes, E. A. (2021). Mapping the Psychosocialcultural Aspects of Healthcare Professionals' Information Security Practices: Systematic Mapping Study. JMIR human factors, 8(2), e17604.

12. [54] Yeng, Prosper Kandabongee, Muhammad Ali Fauzi, and Bian Yang. "Behaviour Coding Approach for Assessing Pitfalls in a Questionnaire Instrument towards assessing healthcare security Practice." (2022).

13. [82] Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. Information, 13(7), 335.

14. [81] Yeng, P. K., Fauzi, M. A., & Yang, B. (2021, November). Assessing the effect of human factors in healthcare cyber security practice: An empirical study. In 25th Pan-Hellenic Conference on Informatics (pp. 472-476).

15. [89] Yeng, P. K., Yang, B., Pederson, M. S., Assessing cyber-security compliance level in paperless hospitals: An ethnographic approach (In press: and presented at The 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2022),Milan, Italy. November 29th - December 1st, 2022)

1.7.1.5 List of contributions in incentivization aspect (Part V)

16. Yeng, P. K., Yang, B., Fauzi, M. A., Nimbe, P., & Priharsari, D., A Framework for Assessing Motivational Methods Towards Incentivizing Cybersecurity Practice in Healthcare (In press: presented at 2022 7th International Conference on Sustainable Information Engineering and Technology)

17. [1] Yeng, P. K., Yang, B., Fauzi, M. A., Vestad A., De Moor, K.R., Jacobsen, C., Exploring cognitive dissonance towards mitigating phishing susceptibility in healthcare: A controlled experiment based on phishing simulation attack in an actual hospital (Under review: Technology in society journal)

1.7.1.6 List of additional research publications not included

1. [77] Yeng, P., Yang, B., Solvoll, T., Nimbe, P., & Weyori, B. A. (2019). Web Vulnerability Measures for SMEs.

2. [62] Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: a systematic literature review. Computer Science Review, 45, 100496.

3. [75] Yeng, P., Woldaregay, A. Z., & Hartvigsen, G. (2019). K-cusum: Cluster detection mechanism in edmon.

4. [22] Elezaj, O., Yayilgan, S. Y., Abomhara, M., Yeng, P., & Ahmed, J. (2019, September). Data-driven intrusion detection system for small and medium enterprises. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-7). IEEE.

5. : [79] Yeng, P. K., Wolthusen, S. D., & Yang, B. (2020). Comparative analysis of software development methodologies for security requirement analysis: towards healthcare security practice. Information Systems (Sofia).

6. [88] Yeng, P. K., Wulthusen, S. D., & Bian, Y. (2020). Comparative Analysis of Threat Modeling Methods for Cloud Computing towards Healthcare Security Practice. International Journal of Advanced Computer Science and Applications, 11(11).

7. [48]Nweke, L. O., Yeng, P., Wolthusen, S., and Yang, B. (2020). Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices.

1.7.2 List of major contributions

In this section, the contribution made in each of the included papers is highlighted and presented in their respective parts of the study and in relation to how they answered the specified research question. However, two of the articles that intersected in all four areas of the study (data-driven, attack and defence, PSC approach, and incentive methods) have also been presented in part I (1.7.2.1).

1.7.2.1 Initial review that intersected all parts of the study (part I)

1. **Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development:**

   This paper addressed issues of in-comprehensiveness in considering the legal requirements for analyzing healthcare security practices in Norway, Ghana, and Indonesia. This has become necessary, as there have been initiatives to assess the security practices of health care staff in these countries. The problem is that there is no comprehensive and

state-of-the-art study of the legal requirements of information security practice that can serve as a baseline for assessing the security practice in health care. A random and non-systematic approach to adopting legal information security requirements in real studies could leave some gaps which can undermine the quality of a study. The contributions in this paper, therefore, include

- The adoption of a comprehensive, and systematic scoping review approach to establish our baseline of legal requirements for future empirical studies.
- Several security requirements, covering data processing, right of access, security by design, access control, email processing, logging, password use, encryption, and health care data storage, were identified and assessed in this work.
- In addition, approximately 80 privacy requirement categories were identified which include consent, disclosure of health data, privacy by design, right to privacy, right of access, data protection, data processing, and personal data.
- A framework was further developed based on these findings to guide future studies in analyzing healthcare security practice.

2. **Framework for healthcare security practice analysis, modelling and incentivization:**

   Modelling and analyzing the security practice of healthcare staff requires a holistic approach. Therefore a summary of contributions in this paper includes the following;

   - A literature survey was conducted for frameworks designed for assessing healthcare staff security practices. The identified frameworks were assessed related to the objective of this thesis work. Some gaps were identified in the existing frameworks, which were assessed and analyzed.
   - Based on the analysis of the identified gaps in the identified frameworks, a comprehensive framework for examining the security practice of healthcare staff was developed. This framework was deemed fit for holistic assessment of the healthcare staff security practice, encompassing attack and defence simulations, access log assessment in the form of data-driven, and assessment of psychological, social and cultural factors in addition to work factors termed in this work as PSC.

1.7.2.2 Part II: Data driven

3. **Observational measures for effective profiling of healthcare staffs' security practices:** In this paper, literature relating to healthcare security breaches reports, some top AI systems for healthcare insider threat detection, standards, regulations and legislation, code of conduct and other literature relating to security measures that are required to observe were surveyed. The contribution in this paper includes;

    - Literature survey to comprehensively identify and analyze various security observational measures which include self-authorization, inter-organizational accesses of PHI and ICT readiness.
    - Sources of observing the security practices were as well identified and analyzed in this work. These sources were assessed to include network logs, browsing history and EHR logs
    - The study results served as a foundation for further studies since the observational measures that were identified are deemed to be of high level and required further and better analysis.

4. **Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review:** In an effort to understand the security susceptibility among healthcare staff, a systematic review was conducted in this paper in the area of data-driven. The basses are that healthcare staff security practices can be traced in various systems' logs in which they accessed. These logs can be processed and analyzed to reveal the user patterns that are associated with the individual staff's security behaviour. The contribution in this work are as follows;

    - Identification and assessment of comprehensive machine learning methods used for modelling and analysing healthcare staff security practice. This provided knowledge on the state-of-the-art machine learning methods and their application and evaluation in analysing healthcare staff security practices.
    - In assessing and considering these machine learning methods, gaps in their application were identified. For instance, supervised learning methods are limited in detecting security practices in scenarios where the logs are unlabeled.
    - The type of logs often used in assessing the security behaviour of healthcare staff were also comprehensively identified, compared and assessed to provide knowledge and direction on their usage for security practice analysis.

- In this paper existing literature in the context of AI for analyzing healthcare staff security practice was also explored to identify limitations and gaps for consideration in this HSPAMI thesis.
- This paper also contributed to providing future direction regarding the application of the identified methods for analyzing healthcare staff security practice.

5. **Artificial Intelligence–Based Framework for Analyzing Health Care Staff Security Practice: Mapping Review and Simulation Study:** Based on the earlier review work in article 4, a framework was developed to provide knowledge on how to efficiently model and analyze logs for assessing security practices among healthcare staff. Following that three models were developed for assessing and analyzing the security practices of the healthcare staff in different scenarios. Several contributions in this paper are as follows;

   - A framework was developed to provide holistic direction as to how to analyze the security practices of healthcare staff, using logs from various sources in healthcare.
   - Three models were subsequently developed to include a) a 3-stage model, b) a 2-class model and c) a 3-class model. This helped in illustrating various scenarios of determining the security practice of healthcare staff.
   - Following the difficulty in obtaining healthcare record logs to evaluate these models, the study further contributed to simulating EHR logs. The simulated logs were used in assessing the identified machine-learning algorithms.
   - How to use various machine learning methods to determine the user's security behaviour was demonstrated. Nine machine learning algorithms were experimented with these models and assessed the performances of these algorithms.

6. **Comparative analysis of machine learning methods for analyzing security practice in electronic health records logs.**

   Based on a variety of machine learning methods that were identified in a systematic review in 4, a comparative analysis of these machine learning algorithms was performed. In summary, the contributions of this paper include;

   - formulation of two role-based anomaly detection models. These were named hard-classification and soft-classification models. The soft-classification model was designed to tolerate healthcare staff to play other functions in other roles, while the hard-classification

model does not provide such tolerance. The hard classification computed for the probabilities of each daily accumulated activity and classified the most probable into the respective role. But, the soft classification adopted a thresh holding mechanism. So if the probability of accumulated daily activities of a user meets a given threshold, that activity is then assigned to the given role.

- Several classification algorithms including KNN, SVM, and decision tree were assessed with these models
- Furthermore assessment of these algorithms based on data normalization methods of these algorithms were compared.

7. **Work flow-based anomaly detection using machine learning on electronic health records' logs: A Comparative Study:**

   In this paper, a model based on the workflow of healthcare staff was developed. The challenge is that broad access is often given to healthcare staff to provide unrestricted access in case of emergency situations. However, this broad access can be abused. Therefore, a model based on the workflow of a typical hospital was developed and used to detect atypical behaviour in EHR logs. Highlights of the contributions in this paper therefore include;

   - Gaps in related studies were identified assessed and analysed through a review of related work.
   - The development of a workflow model to demonstrate how anomaly can be detected in a typical hospital
   - Additionally, several machine learning algorithms were assessed to provide knowledge of how they perform.
   - The performance of the algorithms was also assessed in normalized and non-normalised data sets where random forest attained the best results with normalised data.

8. **Analysing digital evidence towards enhancing healthcare security practice: The KID model:**

   The use of Logs of EHR for analyzing security practices can be challenging especially when the data is unlabelled. The contribution in this paper include;

   - The exploration of related work to ascertain the challenges that are associated with analyzing unlabeled logs for security practice.
   - A model was then developed having combined K-means clustering and iteration discriminate approach. So this piece of work demonstrated that combining K-means clustering with iteration and discrimination can be adopted to analyse security practice with the unsupervised method.

- an evaluation of the clusters with the Silhouette method was performed to provide knowledge on the performance of the various clusters.
- A security malpractice where healthcare staff's average session far exceeded their expected session time was identified. This could imply that healthcare staff were sharing their authenticated sessions.
- The findings in this work can also be used to label features for real-time supervised learning functions.

1.7.2.3 Part III: Attack and defence simulation

9. **Investigation into Phishing Risk Behaviour among Healthcare Staff:** Following the high data breaches through phishing attacks, this paper simulated an SMS-based phishing attack. The targets were two hospitals and their healthcare staff participants, who voluntarily joined the study. Several contributions that were made in this work are as follows;

    - The study identified and assessed phishing simulation tools, and types of phishing susceptibility studies in healthcare. Having assessed these tools, none of them was designed to be suitable for SMS-based phishing attacks. So a system was developed with python-Django api. This was used in combination with SMS service in simulating how an SMS attack can be performed.
    - Ethical dilemmas surrounding in-the-wild-field study in phishing simulation attacks were extensively delved into, through an extensive literature review.
    - SMS-based phishing simulation attack was used in this simulation attack. This is the first of its kind in healthcare research in phishing simulation. Security gaps were then identified having analyzed the results of participants who were victims in the simulation attack and those who were not victims.
    - An interview was used to assess the reasons why some of the participants were victims and why some were not susceptible. This provided knowledge that can be Incorporated in training staff
    - Work factors including workload and work emergency were also analyzed in relation to perception constructs. In this paper, we outlined how management can influence these constructs to enhance security practices.

1.7.2.4 Part IV: Psychological, social, cultural and work factors (PSC) approach

10. **Healthcare staffs' information security practices towards mitigating data breaches: a literature survey:**.

    In this paper, a literature survey was conducted to explore theories and evaluation strategies that can be used to efficiently assess the security practices of healthcare staff. A gist of the contribution is outlined below:

    - Related studies were reviewed to identify various theories and methods that can be used to examine security practice. some of these theories were identified to include HBM, SC, PMT, TPB and the big five (TBF) theory. In the assessment of these theories, comprehensive staff characteristics were identified the psycho-socio-cultural and socio-demographic traits
    - Furthermore, Gaps in the related studies were also identified and assessed and that provided knowledge to combine a number of theories such as HBM, SC, TBF, PMT and TPB to obtain the needed healthcare staffs' characteristics for the study.
    - From this paper, common security practices required by the healthcare staff were also identified and assessed.
    - Moreover, the variety of methods often used in assessing the security practice of healthcare staff in the aspect of PSC, were as well identified and assessed. These include questionnaires, interviews and observation of security practices

11. **Mapping the Psychosocialcultural Aspects of Healthcare Professionals' Information Security Practices:**

    This paper extended the work in article 10. So this paper analysed various frameworks that have been developed in the PSC area. The findings showed that the existing frameworks were not comprehensive for analysing all the factors within this thesis scope. So this paper's contributions include;

    - The adoption of scoping review approach to study various frameworks revealed that these frameworks were developed for assessing social constructs or cultural factors or psychological constructs in isolation. Meanwhile, security issues are influenced by all these factors.
    - Through the extensive literature review, we used an ontology approach to systematically organize the concepts.

- Through the concepts and limitations in these existing frameworks, a comprehensive framework was developed to incorporate multifaceted constructs such as psychological, social, cultural, work factors and socio-demographic.

12. **A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals:**

    Following the framework that was developed in article 11, an empirical study was conducted to assess the security practices of hospitals that fully adopted EHR systems in their operations. The contribution in this paper includes

    - The assessment of security practice knowledge (ISK), attitude (ISA) and behaviour (ISCCBB) with psycho-socio-cultural factors, individual factors and work factors. The findings showed that work emergencies, ISK risks, and ISA risks have a significant positive correlation with self-reported ISCCB risks. From the aspect of psycho-sociocultural behaviour, the study showed that healthcare staff with higher scores in agreeableness, openness and hospital information security culture tend to, respectively, have low cyber security risk behaviour in ISK and ISA, social bonding and response efficacy as well as punishment severity. However, consciousness correlated with high risks of information security-conscious care behaviour.
    - Based on this work, management for instance can design and implement security mitigation strategies in emergency rooms to reduce related susceptibility.

13. **Assessing the effect of human factors in healthcare cyber security practice: An empirical study:** In this article, we examined possible security gaps between the information security (IS) practices of healthcare staff and the security requirement. It was presumed that possible security gaps are caused by poor work factors, personality, psychological, social and cultural perception issues. The contribution of this paper includes the following;

    - A statistical survey was conducted with three departments in a typical hospital to assess a broad range of these factors. From the findings, the healthcare staff' IS knowledge and their self-reported IS conscious care behaviour (ISCCB) showed a gap in their security practices. About half of the respondents' responses were in a higher-risk region. In exploring the reasons for these gaps, the significant effects of the various factors were revealed.

- The paper further suggested possible mitigation strategies and future directions based on the findings. For example, as the study showed security culture to be a predictor of perceived vulnerability risk and punishment severity risk, intrinsic and extrinsic incentives were suggested to influence staff security behaviour.

14. **Qualitative assessment of healthcare staff security practice in paperless hospitals :**

    In this paper, the healthcare staff of some hospitals in Ghana were directly observed and interviewed to assess their security practice. This resulted in the following contribution:

    - The application of both focused group interviews and direct observation to identify and assess healthcare staff security practice. In efforts towards encouraging security practices in healthcare, there was the need to use a qualitative approach in the assessment and analysis of the security practices. This augmented the quantitative approach that was adopted in 12 and 13 in this thesis. Among others, various security practices were discussed. Participants shared their experiences, knowledge, and perception in relation to security policy compliance.
    - From the study, peer pressure and harassment from colleagues, self-seeking interest, and undermined security practices were some of the identified issues that hinder the security practice. Besides, the lack of adoption and use of security governance tools such as information security policy exhibited a fundamental weakness in the security practice foundation in these hospitals. Suggestions based on this study were made to serve as a solution towards enhancing the security practice of the staff.

15. **Pitfalls to watch while designing and pretesting questionnaire for analyzing healthcare security practice: Experience from an empirical study:**

    Due to IT knowledge gaps across the categories of healthcare staff within the scope of IT and information security, developing a questionnaire to effectively assess the security practice while reducing the response burden, was a bit problematic. The contribution in this study is in different facets:

    - Questionnaire response issues were holistically identified and analysed through a review of related work.
    - Additionally, questionnaire design and assessment methods were identified and analyzed. The identified methods include rational,

prototypical, facet, construct, internal and external methods. Additionally, the pretesting methods which were identified include a conventional, cognitive interview, behaviour coding, debriefing, response latency, vignettes, experimental, focus groups, and expert

- Furthermore, the pretesting methods were accessed based on their comparative analysis for effective pretesting of questionnaires towards healthcare security practice.
- Lack of understanding of healthcare information systems' structure, security and privacy concerns of respondents, the insignificant difference between questions, unclear items, complex questions, unrelated questions to respondents and incomplete response options were some of the pitfalls that were identified with a behaviour coding exercise.

1.7.2.5 Part V: Incentivization approach

16. **A framework for incentivising security practice in healthcare:**

    The contributions in this paper are outlined below;

    - A literature survey method was employed to identify and assess various intrinsic and extrinsic motivational methods such as cognitive dissonance, perceived severity, perceived vulnerability and the use of financial reward. Gaps in the existing literature were also analysed in the context of healthcare.
    - Through the literature survey, observational study, and control-experiment were also identified as methods that can be used to assess the efficacy of various motivational methods for incentivising security practice.
    - Following the gap analysis, a framework was developed where a control experiment model can be used to assess the effectiveness of motivation methods for incentivising security practice. This framework was used to examine the effectiveness of cognitive dissonance in a phishing simulation exercise in article 17.

17. **Exploring cognitive dissonance towards mitigating phishing susceptibility in healthcare: A controlled experiment based on phishing simulation attack in an actual hospital:**

    In this paper, a controlled experiment was conducted with a phishing simulation attack to determine the effectiveness of cognitive dissonance towards incentivising good phishing security practices of healthcare staff. The contributions in this work include;

- The design of an email-based control experiment model with cognitive dissonance theory.
- The model was used to assess the actual and self-reported phishing security behaviour of participants. So the susceptibility level of participants in the area of email-based phishing attacks was determined.
- Additionally, knowledge of the influence of cognitive dissonance on the behaviour of participants in both the control group and experiment group was established. Furthermore, perception constructs such as cues to action and perceived severity variables showed that they can be combined with cognitive dissonance to effectively motivate phishing security practices.

1.8 Recommendations for future work

The various research domains in this thesis work (the attack and defence simulation, data-driven approach, and the psychological, social, work and cultural (PSC) factors) can be extended in the future.

In the aspect of attack and defence simulation, there is the need to continue to assess the staff's social engineering resilience while examining other psychological factors that can serve as incentives. For instance, in this thesis work, the study delves much into the phishing attack aspect of social engineering where SMS-based and email-based attack simulations were assessed. Meanwhile, phishing attack also includes other forms of attack such as voice-based, which was not investigated. Besides, the existing literature that was reviewed in the context of healthcare, in this work revealed that voice-based phishing simulation attach have not been experimented with, and this is open for future investigation. Furthermore, in addition to a phishing attack, social engineering attacks include tailgating, the act of an attacker seeking entry to a restricted area, by hiding behind or impersonating a person who has legitimate access. [60]. Such susceptibility in healthcare needs to be investigated in healthcare to provide knowledge for effective security measures. Aside from these, a comprehensive review of phishing simulation attack tools revealed that there is a lack of a comprehensive tool for simulating SMS-based attacks. This challenge motivated the development of a web-based system to complement SMS providers in developing in this thesis. Therefore, there is a need to systematically develop an SMS-based phishing attack simulation platform in future works in contribution to the effective assessment of phishing susceptibility.

Within the aspect of data-driven, host-based logs and network-based logs were not modelled and analyzed to measure the security risks in these aspects. Future works can delve into that by combining various strategies

including modelling and observing user change behaviour in a typical hospital. Due to the limited number of computing resources, healthcare staff tend to share a pool of computers. This means for instance healthcare staff tend to share a single computing or mobile device. How do they manage the use of shared computers without violating security policies, such as password sharing, session sharing and privacy leakage of patients? A systematic approach is required to model and investigate such security practices for improved security practices.

In the aspect of assessing for better incentives towards enhancing security practice, different strategies are required to experiment. As the current work adopted a control experiment where the experiment group was exposed to cognitive dissonance in a questionnaire, alternative approaches such as the use of virtual, augmented and extending realities can be adopted in control experiment studies. These cutting-edge technologies may better induce long-lasting intrinsic or psychological motivation such as perceived susceptibility, self-efficacy, cognitive dissonance issues and perceived severity in healthcare staff.

1.9 Conclusion

Hacking into healthcare IT systems often requires bypassing the organizations' technical security control systems, such as firewalls and intrusion detection systems (IDSs). With heightened technical solutions over the years, circumventing technical measures is often time-consuming and expensive. As a result, cyber adversaries have rather tend to pursue and target "system users", such as the healthcare staff, who are deemed the weakest link in the security chain. As a result, the human element in general has consistently contributed to over 80% of global data breaches, of which healthcare has been one of the most targeted sectors. This thesis work in the HSPAMI project, therefore, contributed towards averting the human susceptibility to security issues in healthcare. This was achieved by modelling, and analyzing healthcare staff security practices.

Based on literature review studies three approaches were adopted in this thesis. These include the data-driven approach, attack and defence simulation and the assessment of psychological, social, cultural and work factors. Within the area of data-driven, the healthcare staff security practices were assessed by modelling and analyzing their self-generated logs through the use of various machine learning methods on simulated EHR logs and real logs from a typical hospital. This was achieved after having analyzed and developed several frameworks and models through in-depth state-of-the-art studies. For instance, the adoption of K-means clustering with iterative and discriminate clustering, revealed unusual session duration in which an average session of about 12,330 hours was detected, while at maximum, a

healthcare staff's session is estimated to be about 24 hours. Essentially, the model predicted normal security practices where a cluster with the maximum login during was about 2 hours. Aside from the identified security gaps in terms of session duration, the findings in the K-Means Iterative and Discriminate(KID) model could be explored towards labelling the log data for real-time abnormal detection and prevention of data breaches.

Additionally, the security practices of healthcare staff were assessed through SMS-based phishing simulation attacks. These attacks were performed having analysed and modelled scenarios through literature review work and observational measures. Through the literature reviews, lab-based phishing experiments, self-reported phishing security practices and in-the-wild-field studies were identified as the most commonly used approach to understanding the susceptibility level of healthcare staff's phishing security behaviour. Out of these methods, the in-wild-field study was considered the most reliable and effective in assessing the phishing susceptibility practice. As a result, we adopted an in-the-wild-field study approach to perform a simulated SMS-based attack in a typical hospital. From a total of 167 participants (comprising nurses, doctors and other healthcare staff), about 101 (61%) were victims of the attack. This trend of a high number of victims in a phishing attack was also identified in a related study in this work in which email was used. Out of about 830 healthcare staff who were targeted with the email-based randomised control experiment with cognitive dissonance, over 50% of the participant fell victim to the attack. Meanwhile, a cyber adversary might need just one person to click the malicious link in a real attack. The higher susceptibility among healthcare staff to the phishing attack, therefore, poses a higher phishing security behaviour risk within the healthcare sector.

Furthermore, several psychological, social, cultural, personal and work-related factors were identified, assessed and analyzed through in-depth literature reviews. Based on that, a comprehensive framework was developed in which several models were created and investigated. Through that, variables such as agreeableness were assessed to be a significant positive predictor of self-efficacy (SE) risk and perceived severity (PS) risks. This means that healthcare workers with agreeable characters tend to have high-risk behaviour in terms of SE and PS. Conscientiousness and neuroticism also had a significant positive correlation with cues to action. This implies that higher risks of cues to action behaviour corresponded to staff who have higher scores in neuroticism and conscientiousness traits. Observing from the results, psychological perceptions in relation to individual factors, such as personality, can be influenced by state-of-the-art training, education and learning (TEL) to improve security practice.

Following the revelation of varying security practice gaps, originating from multifaceted factors in the assessments, cognitive dissonance theory,

together with other incentive methods, were identified and examined in a control-group experiment. The findings in the control experiment showed less susceptibility risk of the actual phishing click behaviour among the healthcare staff in the experiment group. Therefore, cognitive dissonance could be adopted by management in their effort towards mitigating phishing vulnerabilities in the human aspect. Furthermore, as perceived severity exhibited the propensity towards reducing phishing susceptibility amidst cognitive dissonance, management could also be guided by this knowledge to inculcate the potential severity of a potential phishing attack. Cues-to-action measures in combination with cognitive dissonance could also be the game changer. Therefore, the management of various hospitals could combine social engineering-related TEL with psychological incentives such as cognitive dissonance to reduce phishing susceptibility among healthcare staff. For better instilling psychological incentives among healthcare staff, management could ride on state-of-the-art training, education and learning technologies such as virtual reality including extended, or mixed realities.

1.10 Bibliography

[1] Exploring cognitive dissonance towards mitigating phishing susceptibility in healthcare: A controlled experiment based on phishing simulation attack in an actual hospital. 20, 21, 22, 24

[2] Nthe untold story of a cyberattack, a hospital and a dying woman, 2022. Available from: "https://www.wired.co.uk/article/ransomware-hospital-death-germany". 1

[3] OMSORGSDEPARTEMENTET . How does personality influence your cyber risk?, 2021. https://www.cybsafe.com/community/blog/how-does-personality-influence-your-cyber-risk/. 10, 410

[4] ABAWAJY, J. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology 33*, 3 (2014), 237–248. 10, 408

[5] ABDELHAMID, M., ET AL. The role of health concerns in phishing susceptibility: Survey design study. *Journal of medical Internet research 22*, 5 (2020), e18394. 15, 272, 284, 285, 297, 491

[6] AJZEN, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of applied social psychology 32*, 4 (2002), 665–683. 12

[7] AJZEN, I., AND MADDEN, T. J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology 22*, 5 (1986), 453–474. 9, 12, 407

[8] ALBRECHTSEN, E. A qualitative study of users' view on information security. *Computers & security 26*, 4 (2007), 276–289. 10, 408

[9] ANSARI, Z. M., YASIN, H., ZEHRA, N., AND FAISAL, A. Occupational stress among emergency department (ed) staff and the need for investment in health care; a view from pakistan. *Journal of Advances in Medicine and Medical Research* (2015), 1–9. 11, 273

[10] BERGIN, D. L. Cyber-attack and defense simulation framework. *The Journal of Defense Modeling and Simulation 12*, 4 (2015), 383–392. 19

[11] BODDY, A., HURST, W., MACKAY, M., AND EL RHALIBI, A. A study into detecting anomalous behaviours within healthcare infrastructures. In *2016 9th International Conference on Developments in eSystems Engineering (DeSE)* (2016), IEEE, pp. 111–117. 12, 15, 200, 227, 228

[12] BODDY, A. J., HURST, W., MACKAY, M., AND EL RHALIBI, A. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 13, 15, 147, 148, 200, 201, 217, 227, 228

[13] BORDENS, K., AND ABBOTT, B. B. *Ebook: Research Design and Methods: A Process Approach*. McGraw Hill, 2014. 15

[14] CANNOY, S. D., AND SALAM, A. A framework for health care information assurance policy and compliance. *Communications of the ACM 53*, 3 (2010), 126–131. 12, 199, 200, 217

[15] CHA, S.-C., AND YEH, K.-H. A data-driven security risk assessment scheme for personal data protection. *IEEE Access 6* (2018), 50510–50517. 18

[16] CHAMPION, V. L., SKINNER, C. S., ET AL. The health belief model. *Health behavior and health education: Theory, research, and practice 4* (2008), 45–65. 9, 272, 496

[17] CHAUDHRY, J. A., CHAUDHRY, S. A., AND RITTENHOUSE, R. G. Phishing attacks and defenses. *International Journal of Security and Its Applications 10*, 1 (2016), 247–256. 19, 297

[18] CHEN, Y., NYEMBA, S., ZHANG, W., AND MALIN, B. Specializing network analysis to detect anomalous insider actions. *Security informatics 1*, 1 (2012), 1–24. 13, 15, 200, 202, 217

[19] CHENG, L., LI, Y., LI, W., HOLM, E., AND ZHAI, Q. Understanding the violation of is security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security 39* (2013), 447–459. 10, 412, 428

[20] COCKER, F., AND JOSS, N. Compassion fatigue among healthcare, emergency and community service workers: A systematic review. *International journal of environmental research and public health 13*, 6 (2016), 618. 11, 273

[21] COOLICAN, H. *Research methods and statistics in psychology*. 2017. 18, 20, 483

[22] ELEZAJ, O., YAYILGAN, S. Y., ABOMHARA, M., YENG, P., AND AHMED, J. Data-driven intrusion detection system for small and medium enterprises. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (2019), IEEE, pp. 1–7. 25

[23] FERNANDEZ-ALEMAN, J. L., SANCHEZ-HENAREJOS, A., TOVAL, A., SANCHEZ-GARCIA, A. B., HERNANDEZ-HERNANDEZ, I., AND FERNANDEZ-LUQUE, L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics 84*, 6 (2015), 454–467. 12, 15, 200, 406, 414, 415

[24] FISHER, L. E. *The great wall of China*. Simon and Schuster, 1995. 2, 490

[25] GORDON, W. J., WRIGHT, A., AIYAGARI, R., CORBO, L., GLYNN, R. J., KADAKIA, J., KUFAHL, J., MAZZONE, C., NOGA, J., PARKULO, M., ET AL. Assessment of employee susceptibility to phishing attacks at us health care institutions. *JAMA network open 2*, 3 (2019), e190393–e190393. 11, 14, 15, 200, 272, 280, 284, 285, 297, 298, 492

[26] GORDON, W. J., WRIGHT, A., GLYNN, R. J., KADAKIA, J., MAZZONE, C., LEINBACH, E., AND LANDMAN, A. Evaluation of a mandatory phishing training program for high-risk employees at a us healthcare system. *Journal of the American Medical Informatics Association 26*, 6 (2019), 547–552. 14, 15, 200, 272, 284, 285, 297, 491, 492

[27] GRATIAN, M., BANDI, S., CUKIER, M., DYKSTRA, J., AND GINTHER, A. Correlating human traits and cyber security behavior intentions. *computers & security 73* (2018), 345–358. 10, 410

[28] GUO, K. H. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security 32* (2013), 242–251. 1

[29] HAWORTH, J. Uk government employees receive 'billions' of malicious emails per year – report, April 2022. Available from: https://portswigger.net/daily-swig/uk-governmentemployees-receive-billions&-of-malicious-emails-per-year-report. 1, 454, 490

[30] HERATH, T., AND RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems 47*, 2 (2009), 154–165. 7, 405, 412, 428, 448, 457, 493

[31] HEVNER, A. R., MARCH, S. T., PARK, J., AND RAM, S. Design science in information systems research. *MIS quarterly* (2004), 75–105. 20

[32] HUGHES, O. Norway healthcare cyber-attack 'could be biggest of its kind, 2022. Available from: "https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/". 1

[33] HUMAIDI, N., AND BALAKRISHNAN, V. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR* (2012), vol. 35, IACSIT Press Singapore, pp. 1–6. 12, 15, 200, 272, 274

[34] HUMAIDI, N., BALAKRISHNAN, V., AND SHAHROM, M. Exploring user's compliance behavior towards health information system security policies based on extended health belief model. In *2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)* (2014), IEEE, pp. 30–35. 9, 273, 274, 496, 509

[35] IFINEDO, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security 31*, 1 (2012), 83–95. 10, 273, 457, 496

[36] ISO. 27799:2016(en), health informatics information security management in health using iso/iec 27002. 2016., November 2016. 2, 6, 198

[37] ISO. Iso/iec 27005:2018 information technology — security techniques — information security risk management., November 2018. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en. 7

[38] JALALI, M. S., BRUCKES, M., WESTMATTELMANN, D., AND SCHEWE, G. Why employees (still) click on phishing links: investigation in hospitals. *Journal of medical Internet research 22*, 1 (2020), e16775. 11, 15, 272, 273, 274, 280, 282, 284, 285, 295, 296, 297, 299, 312, 313, 445, 491, 492, 508

[39] KAFKA, F. The great wall of china. *Commentary 2* (1946), 368. 2, 490

[40] KOTHARI, C. R. *Research methodology: Methods and techniques*. New Age International, 2004. 15

[41] KUECHLER, B., AND VAISHNAVI, V. On theory development in design science research: anatomy of a research project. *European Journal of Information Systems 17*, 5 (2008), 489–504. 20

[42] LEONARD, L. N., CRONAN, T. P., AND KREIE, J. What influences it ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management 42*, 1 (2004), 143–158. 9, 408

[43] MCCORMAC, A., ZWAANS, T., PARSONS, K., CALIC, D., BUTAVICIUS, M., AND PATTINSON, M. Individual differences and information security awareness. *Computers in Human Behavior 69* (2017), 151–156. 10, 410

[44] MINISTRY OF CULTURE, P. The great wall of china, November 2009. Available from: `http://en.chinaculture.org/focus/focus/2010expo_en/2010-04/19/content_376769_3.html`. 2, 490

[45] MOU, J., COHEN, J. F., BHATTACHERJEE, A., AND KIM, J. A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems 23*, 1 (2022), 196–236. 10, 273, 457, 496

[46] NAKANO, H., CHIBA, D., KOIDE, T., AKIYAMA, M., YOSHIOKA, K., AND MATSUMOTO, T. Exploring event-synced navigation attacks across user-generated content platforms in the wild. *Journal of Information Processing 30* (2022), 372–387. 14

[47] NG, B.-Y., KANKANHALLI, A., AND XU, Y. C. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 4 (2009), 815–825. 9, 271, 272, 273, 296, 313, 442, 496, 509, 512

[48] NWEKE, L. O., YENG, P., WOLTHUSEN, S., AND YANG, B. Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices. 25

[49] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., AND ZWAANS, T. The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security 66* (2017), 40–51. 10, 278, 404, 405, 406, 408, 413, 414, 415, 426, 428, 443, 446, 499, 501, 502

[50] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. The development of the human aspects of information security questionnaire (hais-q). 7, 10, 278, 282, 414, 442, 443, 446, 461, 498

[51] PAUL III, D. P., SPENCE, N., BHARDWA, N., PH, C. D., ET AL. Healthcare facilities: another target for ransomware attacks. 19, 20

[52] PEFFERS, K., TUUNANEN, T., ROTHENBERGER, M. A., AND CHATTERJEE, S. A design science research methodology for information systems research. *Journal of management information systems 24*, 3 (2007), 45–77. 20

[53] PRIESTMAN, W., ANSTIS, T., SEBIRE, I. G., SRIDHARAN, S., AND SEBIRE, N. J. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics 26*, 1 (2019). 11, 15, 272, 284, 285, 297, 492

[54] PROSPER KANDABONGEE YENG, M. A. F., AND YANG, B. ehaviour coding approach for assessing pitfalls in a questionnaire instrument towards assessing healthcare security practice. In *5th International Conference on Management Science and Industrial Engineering will be held in Chiang Mai, Thailand during* (2023), vol. in press. 22, 24

[55] PROSPER YENG, MUHAMMAD ALI FAUZI, B. Y., AND NIMBE, P. Investigation into phishing risk behaviour among healthcare staff. *MPDI Information 13*, 8 (2022), 392. 19, 20, 21, 490, 497

[56] RAJA, M. C., AND RABBANI, M. A. Big data analytics security issues in data driven information system. *Int J Innov Res Comput Commun Eng 2*, 10 (2014), 6132–5. 18

[57] RENAUD, K., AND GOUCHER, W. Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security* (2012). 2, 6, 454, 457

[58] RIZZONI, F., MAGALINI, S., CASAROLI, A., MARI, P., DIXON, M., AND COVENTRY, L. Phishing simulation exercise in a large hospital: A case study. *Digital Health 8* (2022), 20552076221081716. 2, 11, 14, 15, 454, 490, 492, 506

[59] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 9, 10, 12, 15, 200, 274, 405, 407, 412, 428, 446, 457

[60] SALAHDINE, F., AND KAABOUCH, N. Social engineering attacks: A survey. *Future Internet 11*, 4 (2019), 89. 35

[61] SHROPSHIRE, J., WARKENTIN, M., AND SHARMA, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *computers & security 49* (2015), 177–191. 10, 410, 428

[62] SHUKLA, A., KATT, B., NWEKE, L. O., YENG, P. K., AND WELDEHAWARYAT, G. K. System security assurance: a systematic literature review. *arXiv preprint arXiv:2110.01904* (2021). 25

[63] SLONKA, K. J., AND SHRIFT, B. F. Phishing our clients: A step toward improving training via social engineering. *Issues in Information Systems 17*, 1 (2016). 14, 15, 272, 284, 285, 297, 298, 491

[64] TAYLOR, T. Hackers, breaches, and the value of healthcare data, November 2021. Available from: `https://www.securelink.com/blog/healthcare-data-new-prize-hackers/`. 2

[65] TAYLOR, T. Patient data '10-15 times more valuable than credit card data, November 2021. Available from: `https://www.irishexaminer.com/news/arid-40293149.html`. 2

[66] THIRUMALAI, C., CHANDHINI, S. A., AND VAISHNAVI, M. Analysing the concrete compressive strength using pearson and spearman. In *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)* (2017), vol. 2, IEEE, pp. 215–218. 10, 408, 414

[67] UFFEN, J., GUHR, N., AND BREITNER, M. H. Personality traits and information security management: An empirical study of information security executives. 10, 410, 442

[68] VENKATESHA, S., REDDY, K. R., AND CHANDAVARKAR, B. Social engineering attacks during the covid-19 pandemic. *SN computer science 2*, 2 (2021), 1–9. 2, 454, 490

[69] VERIZON2021. 2021 data breach investigations report, November 2021. Available from: `https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf`. 1, 270, 293, 441, 454

[70] VERIZON2021. 2022 data breach investigations report, September 2022. Available from: https://www.verizon.com/business/resources/reports/dbir/. 1, 454

[71] WEN, Z. A., LIN, Z., CHEN, R., AND ANDERSEN, E. What.hack: Engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), CHI '19, Association for Computing Machinery, p. 1–12. Available from: https://doi.org/10.1145/3290605.3300338. 19

[72] WHITMAN, M. E., FENDLER, P., CAYLOR, J., AND BAKER, D. Rebuilding the human firewall. In *Proceedings of the 2nd annual conference on Information security curriculum development* (2005), pp. 104–106. 1, 329, 331, 340

[73] WHITMAN, M. E., FENDLER, P., CAYLOR, J., AND BAKER, D. Rebuilding the human firewall. In *Proceedings of the 2nd annual conference on Information security curriculum development* (2005), pp. 104–106. 2, 224

[74] WRIGHT, A., AARON, S., AND BATES, D. W. The big phish: cyberattacks against us healthcare systems, 2016. 14, 15, 200

[75] YENG, P., WOLDAREGAY, A. Z., AND HARTVIGSEN, G. K-cusum: Cluster detection mechanism in edmon. 25, 217, 234, 249, 298

[76] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[77] YENG, P., YANG, B., SOLVOLL, T., NIMBE, P., AND WEYORI, B. A. Web vulnerability measures for smes. 24

[78] YENG, P. K., FAUZI, M. A., SUN, L., AND YANG, B. Assessing the legal aspects of information security requirements for health care in 3 countries: Scoping review and framework development. *JMIR Human Factors 9*, 2 (2022), e30050. 3, 22, 465, 468

[79] YENG, P. K., FAUZI, M. A., AND YANG, B. Comparative analysis of machine learning methods for analyzing security practice in electronic health records' logs. In *2020 IEEE International Conference on Big Data (Big Data)* (2020), IEEE, pp. 3856–3866. 22, 23, 25, 247, 248

[80] YENG, P. K., FAUZI, M. A., AND YANG, B. Workflow-based anomaly detection using machine learning on electronic health records' logs: A

comparative study. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)* (2020), IEEE, pp. 753–760. 22, 23, 247, 248

[81] YENG, P. K., FAUZI, M. A., AND YANG, B. Assessing the effect of human factors in healthcare cyber security practice: An empirical study. In *25th Pan-Hellenic Conference on Informatics* (2021), pp. 472–476. 22, 24, 490, 509

[82] YENG, P. K., FAUZI, M. A., AND YANG, B. A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information 13*, 7 (2022), 335. 24, 455, 456, 461, 495, 501, 509

[83] YENG, P. K., FAUZI, M. A., YANG, B., AND NIMBE, P. Investigation into phishing risk behaviour among healthcare staff. *Information 13*, 8 (2022), 392. 22, 23

[84] YENG, P. K., FAUZI, M. A., YANG, B., AND YAYILGAN, S. Y. Analysing digital evidence towards enhancing healthcare security practice: The kid model. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (2022), pp. 1–9. 19, 22, 23

[85] YENG, P. K., NWEKE, L. O., YANG, B., FAUZI, M. A., AND SNEKKENES, E. A. Artificial intelligence–based framework for analyzing health care staff security practice: Mapping review and simulation study. *JMIR Medical Informatics 9*, 12 (2021), e19250. 15, 22, 23, 247, 248, 263

[86] YENG, P. K., SZEKERES, A., YANG, B., AND SNEKKENES, E. A. Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: Systematic mapping study. *JMIR human factors 8*, 2 (2021), e17604. 9, 11, 15, 17, 24, 272, 273, 274, 282, 405, 406, 407, 414, 457, 496, 498

[87] YENG, P. K., WOLTHUSEN, S. D., AND BIAN, Y. Adopting vulnerability principle as the panacea for security policy monitoring. *International Journal of Advanced Computer Science and Applications 12*, 3 (2021). 9

[88] YENG, P. K., WULTHUSEN, S. D., AND BIAN, Y. Comparative analysis of threat modeling methods for cloud computing towards healthcare security practice. *International Journal of Advanced Computer Science and Applications 11*, 11 (2020). 25

[89] YENG, P. K., YANG, B., AND PERDESON, M. Qualitative assessment of healthcare staff security practice in paperless hospitals. 24

[90] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 11, 15, 22, 138, 200, 217, 224, 236, 273, 274, 404, 406, 407, 409, 414, 426, 442, 491, 498

[91] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 1, 2, 6, 10, 11, 15, 17, 23, 199, 217, 224, 274, 282, 404, 405, 406, 407, 409, 410, 414, 442, 443, 454, 457, 491, 498

[92] YENG P, FAUZI MA, S. L., AND B, Y. Legal aspects of information security requirements for healthcare in three countries: A scoping review as a benchmark towards assessing healthcare security practices. *JMIR Hum Factors* (2022). Available from: `https://humanfactors.jmir.org/2022/0/e0/`. 7, 15, 246, 405

[93] YENG, PROSPER KANDABONGEE AND NWEKE, LIVINUS OBIORA AND WOLDAREGAY, ASHENAFI ZEBENE AND YANG, BIAN AND SNEKKENES, EINAR ARTHUR. Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. In *Proceedings of SAI Intelligent Systems Conference* (2020), Springer, pp. 1–18. 11, 19, 23, 200, 201, 202, 217, 247

[94] YURYNA CONNOLLY, L., LANG, M., GATHEGI, J., AND TYGAR, D. J. Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security 25*, 2 (2017), 118–136. 1

Part I

Initial review work

Chapter 2

Legal Aspect of Information Security Requirement for Healthcare in Three Countries: A scoping Review as a Benchmark towards Assessing Healthcare Security Practice

Prosper kandabongee Yeng, Muhammad Ali Fauzi, Luyi Sun, Bian Yang

This paper is awaiting publication and is not included

2019 IEEE International Conference on Big Data (Big Data) https://doi/10.1109/BigData47090.2019.9006529

Chapter 3

Framework for Healthcare Security Practice Analysis, Modeling and Incentivization

Prosper Kandabongee Yeng ; Bian Yang ; Einar Arthur Snekkenes

Abstract

Healthcare professionals are often the weakest link in the security chain, which is contributing to data breaches in the healthcare sector. A number of reasons account for this. Technological countermeasures for cyber defenses have been heightened and the adversaries tend to exploit easy entry points. Besides, healthcare staffs are usually occupied by their core duty of healthcare provison with little experience in information security. With a Design Science Research (DSR), observational measures for effective profiling of healthcare staffs were developed. Regulations and security standards such as the Code of Conduct, General Data Protection Regulation (GDPR) of European Union (EU), ISO 7799, and other Norwegian Acts and regulations for personal data protection, were reviewed for the observational measures. A comprehensive Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) framework was then proposed for analyzing healthcare staffs' security practices in a comprehensive way.

3.1 Introduction

The shift of cyber-criminal activities from the financial institutions to healthcare is threatening the mutual trust and confidentiality between healthcare and patients[16, 18]. The mutual trust between healthcare professionals and patients is very vital for the provision of quality healthcare in society. The healthcare professionals rely on the accuracy and completeness of information given by patients in order to prescribe therapeutic measures for health conditions [12]. As a result, health providers turn to store large quantities of personal sensitive information of patients. In a similar vein, patients trust

that, their personal information which are disclosed for medical reasons are to be kept confidential. This trust has been supported and sealed by various regulatory and legal instruments such as the GDPR, the Health Records Act, the Health Personnel Act, the Personal Health Data Filing System Act, the Health Research Act, and the Patients' and Users' Rights Act [29]. Unfortunately, this mutual trust in relation to patients' data is often broken through cyber-criminal activities. In healthcare data breaches scenarios, the patients records become unreliable for therapeutic purposes and the patient right to privacy is as well trampled upon. Healthcare information has been classified to be among the most confidential of all types of personal data but has recently become the subject of targets. For instance, in 2018, through the aid of a staff, the health care records of about half the total population of Norway (3 million) were compromised [10]. Also, a phishing attack resulted in breaching 38,000 patients records at Portland, Oregon-based Legacy Health in the United State of America [20]. Personal data such as patients' email accounts, demographic information, dates of birth, health insurance data, billing details, medical data, Social Security numbers and driver's licenses were stolen. In a similar incidence [20], about 1.5 million patient records, including data of the prime minister of Singapore, were breached. A front-end workstation was first compromised to get access to privileged user credentials. In the United States, about 365 breaches were reported in 2018 with hacking being the leading cause of healthcare data breaches followed by unauthorized access and disclosure incidents [8]. The Confidentiality, Integrity and Confidentiality (CIA) of healthcare data become compromised in healthcare data breaches situations. Meaning that, the electronic medical records or medical devices cannot be trusted to be accurate for therapeutic measures. For instance, the blood group, prescribed medicines or diagnosis attributes of patients can be changed in compromised healthcare data and rendering it unsafe for therapeutic purposes. Resent ransomware attacks in healthcare compromised the availability of the healthcare records for medical care.

Aside economic losses, loss of trust and privacy issues, data breaches may result in loss of human lives, carding sites, fake documentation services, drugs, weapons and pharmaceuticals [22, 25]. The healthcare organization may also face stringent sanctions from regulatory bodies such as the (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) [22]. Violations of privacy and security regulations by organizations could result in fines up to 4% of their annual global turnover or Twenty Million Euros [10]. According to the international standard organization (ISO), the annual estimated losses from cybercrime could reach USD 2 trillion in the near future. In addition, there will be countless daily additions of new breaches [20]. In the midst of these problems, healthcare security practice analysis, modeling and incentivization (HSPAMI) project was initiated and

operated by the Centre of Cyber and Information Security of NTNU with funding from the Ministry of Health and Care of Norway to contribute towards mitigating data breaches in healthcare[4, 9].The general objective of HSPAMI is to determine the security gap in healthcare staffs' information security practices in respect to required security practices as outlined in the code of conducts, policies and regulations [29]. The specific objective was to propose a holistic framework towards modeling and analyzing healthcare staffs' security practices. The remaining of this section specifies the research problem and its contribution. Section 4.3.1 presented the state-of-the-art on existing frameworks. The approach of the study was presented in section 4.2 while the findings and framework were presented in section 4.2. Finally, the results were discussed and concluded in section 3.5.

3.1.1 Research problem

A literature survey for appropriate frameworks for modeling and analyzing healthcare staffs' security practices revealed different types. However none of them adopted a holistic approach. Some of the frameworks could be used to evaluate only psychological and socio-cultural context [17, 11, 26]. Other frameworks also focused on only big data or user data logs related analysis[13-15]. Further, other frameworks could only be used for attack and defense scenarios[16-18] as shown in Figure 12.1. Adopting any of these frameworks without a holistic approach is deemed inefficient for effective modeling and analysing healthcare security practices.

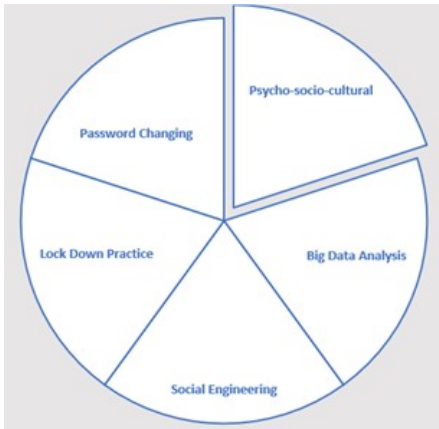


Figure 3.1: Healthcare Security practices

For instance, in a scenario where framework relating to only big data was adopted to obtain outliers. The reasons for the outliers can not be properly

determined unless this is complemented with a qualitative studies such as observations, interviews or open ended questionnaires [30]. Also, an assessment of the perception and socio-cultural security metrics as shown in figure 2.1 would be a partial solution. Because, psycho-socio-cultural context alone may not disclose the social engineering security metrics of healthcare staffs. More to this, an adoption of only attack-defence scenario would help us to possibly train healthcare staffs to be able to identify malicious emails, phone calls or text messages. But if the healthcare staff can not perceive the severity of their security misbehaviors (as specified in Protection Motivation Theory), the healthcare professionals may still not be incentivized to adopt to conscious care behavior.

3.1.2 Contribution

Based on the problems in existing frameworks as indicated in subsection A, the contribution of this study was a proposed comprehensive framework known as HSPAMI framework. This holistic approach was towards addressing the weaknesses of the existing frameworks which were identified in the state-of-the-art studies. In this study, the healthcare staffs refer to healthcare personnel who access patients' records in the discharge of their duties. They include nurses, physicians, psychologists, laboratory personnel and radiology staffs. Therefore, healthcare staffs, healthcare professionals and healthcare workers were interchangeably used in this study. Also, Psycho-socio-cultural context was used in this study to refer to modeling and analyzing perception or psychological, social demographics and socio-cultural variables as defined in Table 12.1.

3.2 State-of-the-art

In an effort towards developing security-conscious care behaviour among healthcare workers, Norshima et al [17], developed a conceptual framework for analyzing the influence of security awareness and security technology on healthcare staffs' security practices. Protection Motivation Theory and Health Belief Model attributes were used as independent variables to determine their impact on the security awareness and security technology mediating variables. Similarly, Cannoy et al., employed the Technology Acceptance Theory(TAM), the Theory of Reasoned Action, information assurance and security ethical behavior, organizational culture and health information management [5]. The frameworks adopted quantitative and qualitative methods, of interviews and questionnaire surveys. While security gaps of psychological traits and ethics are essential, studying and covering security gaps in these aspect alone may only be a drop in the ocean [12, 29, 19]. Fur-

thermore, the security awareness and security technology alone does not constitute significant proportion of healthcare security practices [24].

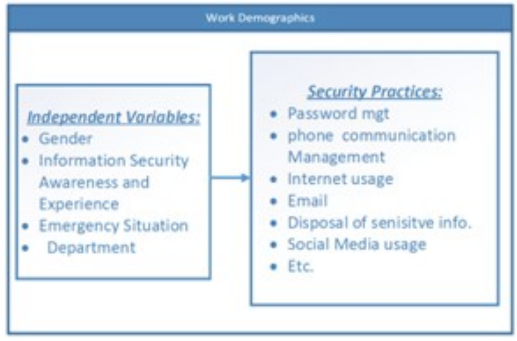


Figure 3.2: Relating Demographic variables with security practices

Additionally, Fernandez-Aleman et al., evaluated the security practices of healthcare staffs in a real clinical setting[11]. Standards, guidelines and recommendations on security and privacy best practices for healthcare staffs were identified in a systematic literature review for the development of a survey questionnaire. 27 questions were developed and used to survey 180 healthcare staffs in a public hospital. In the survey, 62.2% of the respondents reported weak passwords, 31.7% did not know the established procedures for discarding sensitive information, and 19.4% did not carry out these procedures. There were no computer screen shields in place against unauthorized persons and more than half of the respondents did not know of incidence reporting procedure. The correlation between experience and good security practices was insignificant and age was weakly correlated with good security practices.

Fernandez-Aleman et al., advocated for more security awareness training to enhance good security practices and also called for preventive and corrective actions to curtail staffs' security related incidents. Fernandez-Aleman et al., studied into the psycho-socio-cultural context and related some social demographic characteristics (age, gender and experience) with some security practices in password management, unauthorized accesses, disposal of sensitive information and incidence reporting which provided some knowledge on the security gap between healthcare professionals' information security practice and expected practice. However, the study was incomprehensive and lacked most of the needed security gaps. Healthcare security practices is not only impacted by these social demographic traits of age, gender and experience [12, 29, 19]. but could be influenced by other critical factors such as emergency situations or workload as shown in Figure 12.2. The security practices which were analyzed did not cover the rec-

ommended observational measures and security practices [24]. The study did not also include psychological, cultural and some social traits such as believes, perceptions and peer group influence. Fernandez-Aleman et al., studies did not also cover the analysis of big data such as logs and assessment of the resilience of healthcare staffs against some social engineering attacks.

Protection Motivation Theory (PMT) and Theory of Planned Behavior(TPB) [24] were adopted in a study to determine if information security awareness, information security policy and experience have impact on employee security practices. TPB relies on attitude, subjective norms, and perceived behavioral control to influence individual way of life [1, 2]. The PMT is the ability to protect oneself based on; perceived severity of a threatened event, perceived probability of the occurrence, or vulnerability, the impact of the recommended preventive practices and perceived self-efficacy[12]. Experts opinions were used to develop questionnaires based on the PMT and TPB. The questionnaire was used to survey 220 information security experts and professionals in information technology across various industries. The results were positive in terms of Information Security Awareness, Information Security Policy, Information Security Experience and Involvement, Attitude towards information security, Subjective Norms, Threat Appraisal, and Information Security self-efficacy.

A related framework was also conceptually designed and developed by, Boddy et al., in healthcare infrastructure [3]. The framework has a processing model used to process input data from computers and medical devices by eliminating extraneous data. A database component of the framework was used to store the cleaned dataset together with known attack signatures of dataset. The entire stored dataset was purported for comparing with input dataset to detect malicious intentions. The stored dataset was further processed for visualization.

The output of the visualization was designed to be interrupted by the system users by adjusting parameters to achieve the security situational purpose of the infrastructure. In an experimental study of the framework, the active directory domain controller network statistic (netstat) was captured, analyzed and visualized. In the netstat, the connection type (TCP), source and destination IPs and connection states were captured. In the experiment, a security threat was identified through most frequent accesses from foreign IP addresses. Also in an efforts to enhance information security relating to insider misbehaviors, Chen et al., [6] created a network anomaly detection sensor (known as SNAD) to determine when specific practices of an insider significantly deviate from a baseline in a collaborative information system. The study was on the premise that if a healthcare staff practices is an anomaly, the similarity of the network of collaborative staffs' practices will be higher when the anomalous user is suppressed from the network group.

So, a model was developed for each patient's medical record in relation to a group of authenticated healthcare staffs who have related accesses to the subject. A subject-user bipartite graph as a binary matrix was further developed for the similarity measure. The significance of the similarity of the user group with and without the potentially malicious user was determined. SNAD was assessed with access logs of patient record of a large electronic health record system (6,015 users, 130,457 patients and 1,327,500 accesses) and it was comparatively more effective.

Recently, Boddy et al., [4] studied into a Local Outlier Factor (LOF)-based data analytics technique, to analyze Electronic Patients Records (EPRs) data and provided context awareness to spot poor security practices. The statistical variables used included Frequency, Mean, Median, Mode, Standard Deviation, Minimum, Maximum, 1st Quartile, 3rd Quartile features, 5th Percentile and 95th Percentile features of the dataset for each User, Patient, Device and Routine. These variables were processed and used to detect outliers through the measurements of local deviations. A LOF anomaly score was determined for each of the User, Patient, Device and Routine IDs. The anomaly score was determined by measuring the local distance of density and determining how far-away the value was in relation to the k-nearest neighbors. A LOF anomaly score of 1 indicated that an object was comparable to its neighbors and represents an inlier. A value below 1 was considered a dense region, and an inlier, however, a value with significant measure greater than 1 was considered outlier. The algorithm detected 144 outliers in an unlabeled dataset of 1,007,727 audit logs which consisted of 0.66% of the users on the system, 0.17% of patient record accesses, 0.74% of routine accesses, and 0.53% of the devices used in a specialist Liverpool (U.K.) hospital. The frameworks, [3, 6] and [4]only adopted big data analysis approach which is not enough to provide the reasons behind potential outliers.

Using social engineering methods to manipulate healthcare staffs was also analyzed by various studies. According to Wright et al., social engineering is one of the methods that healthcare staffs often fall victims to, while practicing information security [28]. Social engineering involves phishing-the act of tricking users to obtain their access credentials for illegitimate accesses. The practice often involve manipulation and deceiving legitimate system users to click a link and enter their usernames and passwords. Some users sometimes take the bait and enter their credentials on the hacker's site. This gives the hacker the ability to impersonate the legitimate user and gain unauthorized access to their systems. Clicking of malicious links may also lead to other forms of attacks such as ransomware and cross site scripting. Some phishing attacks target many users while spear phishing attacks involve

targeting an organization, an individual or smaller group. There have been numerous data breaches in healthcare through phishing attack meth-

Table 3.1: Summary of Literature survey.

Framework/Study	HSPAMI Study areas addressed	Approach
A conceptual framework [17]	Users perception	Qualitative, Quantitative
Framework for healthcare information assurance policy and compliance [5]	Users perception	Qualitative
Security practices of healthcare staffs in real clinical setting [11]	Users perception	Survey with questionnaires
Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB)[26]	Users perception	Survey with questionnaires
Conceptual Framework [3]	Big data analysis	Comparison of input data with known attack signatures
Network anomaly detection sensor (SNAD)[6]	Big data analysis	Comparison of input data with established pattern
Network anomaly detection sensor (SNAD) [6]	Big data analysis	Comparison of input data with established pattern
Local Outlier Factor (LOF) in Electronic Patients Records [4]	Big data analysis	KNN
Cyberattacks Against U.S. Healthcare Systems [28]	Social Engineering	Reviews of phishing attacks
Evaluation phishing training program for high-risk healthcare staffs [16]	Social engineering	Phishing Attack-Defense simulation
Assessment of Employee Susceptibility to Phishing Attacks [14]	Social Engineering	Phishing Attack-Defense simulation

ods. The adversaries often search through victim's mailbox for files that contain personally identified information and can escalate privileges to admin level. The motivation of the phishers is mostly to obtain sensitive individuals' information such as date of births, social security numbers, phone numbers and many more. The stolen sensitive data could be sold through online black markets and local criminal networks. Stolen health information can

also be used for other types of fraud including access payroll systems and change salary, change deposit destinations to bank accounts [9], forging prescriptions, blackmailing or other evil purposes. Training, simulated phishing attacks, filtering, frequent password changes, limiting amount of data accesses and multi-factor authentication are some of the mitigation strategie In a related study, Gordon et al., conducted a phishing attack simulation to profile offenders for treatment against phishing attacks in an anonymous US healthcare institution [15].

A phishing email was being sent to a large group of healthcare workers from time to time. Staffs who clicked on at least 5 of the simulated phishing emails before the 16th round of sending the email were labeled as offenders in the study. Out of a total of 5416 unique healthcare staffs who participated fully in the simulation exercise, more than halve of the users clicked on at least 2 of the simulated phishing emails and about quarter of them were profiled as offenders for intervention measures. The offenders were then notified of their susceptibility to phishing attack and were trained on the overview of phishing, phishing scenarios, and how to identify such attacks. Similarly, email phishing was identified as a major attack vector [18] on healthcare staffs in various hospitals.

So, a phishing simulation exercise was conducted between 2011 and 2018 across 6 US health institutions to describe the practice of phishing simulation and the extent to which health care employees are vulnerable to phishing attacks. For security and privacy concerns, the healthcare institutions in the study were anonymized. In 95 simulated phishing campaigns, 2 971 945 phishing emails which were sent resulted in 422 062 (14.2%) clicked. About 1 in 7 simulated emails sent were clicked on by healthcare staffs. The study observed that increasing campaigns were associated with decreased odds of clicking on a phishing email which indicate a potential benefit of phishing simulation and awareness.

As shown in table 12.1, the frameworks [3, 6] and [4] adopted only data analysis approach to measure healthcare staffs' security practices. Similarly, [17, 11] and [26] were related to only psycho-socio-cultural context in relation to staffs' security practices[9]. Furthermore, [28, 15] and [14] obtained information security metrics through analyzing phishing attacks. These studies contributed knowledge in mitigating security violations in their various aspects but none of them adopted a holistic approach. Therefore, the HSPAMI framework aimed towards combining these separated studies into a comprehensive framework.

3.3 Method

A Design Science Research (DSR) approach was adopted in the development of the HSPAMI framework[8, 23]. The study problem was first identi-

fied through literature survey. IEEE-Xplore, Google Scholar, Elsevier and Science Direct were surveyed for journals and conference papers for related frameworks. There was no comprehensive framework for healthcare staffs' security practice analysis, modeling and incentivization among the reviewed literatures. The objective(s) of the intended solution was then designed and developed as shown in Figure 12.3. The results and evaluation of the framework were communicated in the results and discussion sections.

3.4 Results

on the the frameworks which were developed for studying healthcare security practice. The proposed comprehensive framework known as HSPAMI Framework was also presented.

3.4.1 Findings from literature survey

A summary of the literature survey as shown in Table 12.1 were grouped into three categories. Thus psycho-socio-cultural-context, big data analysis of users' access logs and attack-defence scenarios. [17, 11] and [26] studied into the perception and socio-demographic aspect of the psycho-socio-cultural context model of HSPAMI. Social and cultural aspect of the psycho-socio-cultural context were excluded in these studies. [13, 14] and [15] adopted only data analysis approach to measure healthcare staffs' security practices while [28, 15] and [14] explored social engineering methods. None of the reviewed frameworks as shown in Table 12.1, adopted a combination of the various categories towards obtaining a comprehensive information security metrics in healthcare professional security practices.

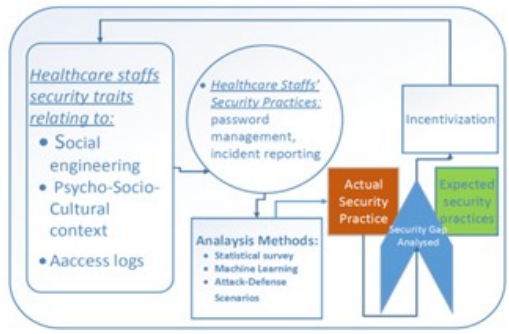


Figure 3.3: Overview of HSPAMI study

3.4.2 Proposed HSMPAMI Framework

Since healthcare staffs are deemed the weakest link in the security chain, the modeling and analysis of their security practices should be comprehensive and iterative towards effective results. So, all related traits which can significantly contribute to security issues need to be identified model and analyzed. The identified traits and security practices can then be studied with the appropriate methods such as statistical surveys, artificial intelligence, attack-defense scenarios and other practical analysis. The overview of HSPAMI study cycle is as shown in Figure 12.3. After the analysis, the gap between the staffs' security practices and required practices is identified. The gap or results obtained would then guide a study into incentivization methods which can be used to influence staffs' security practices towards closing the gap. The study is for building a security culture and security conscious behavior among the healthcare staffs. The HSPAMI framework as shown in Figure 12.4 is an extension of the overview of Figure 12.3, with some details of the various models. The proposed HSPAMI framework has a security gap analysis module which consists of required security practices and actual security practices of healthcare staffs. The required security practice aspect of the framework consists of the expected conscious care behavior of healthcare staffs as defined in legal and regulatory instruments, code of conducts, ethics, information security policies and standards towards preserving the privacy right of patients [29]. The healthcare staffs' security practices model is for the determination of security metrics in psycho-socio-cultural context, attack and defense simulation scenarios and big data analysis of the staffs' accesses with artificial intelligence as shown in figure 12.3. The data analysis aspect constitutes analyzing data sources which contain the security practices of healthcare staffs' in which their unique profile can be created to constitute a non-repudiation of their actions. Such data sources include Network logs, Electronic Health Records (EHR) logs, browsing history, operating system processes' logs among others[12, 29]. These data sources serve as input to the data analysis model. A learning algorithm is used to study and form each healthcare staff's profile from the input source. The profile can then serve as a baseline for observing significant deviations. Having formed the baseline, later activities of the healthcare staff are compared with the established baseline for aberration detection. If there exists an anomaly, a further processing is done in the anomaly analysis model to determine if the anomaly was malicious. Malicious activities are deeply analyzed to determine and classify the type of the malicious activity.

If the activity was determined not to be malicious, the activity is further investigated and the "Build normal profile" was updated if the investigated output of the activity was determined to be false alarm.

The psycho-socio-cultural module relates the healthcare staffs' psycho-socio-cultural security characteristics with the healthcare staffs, security prac-

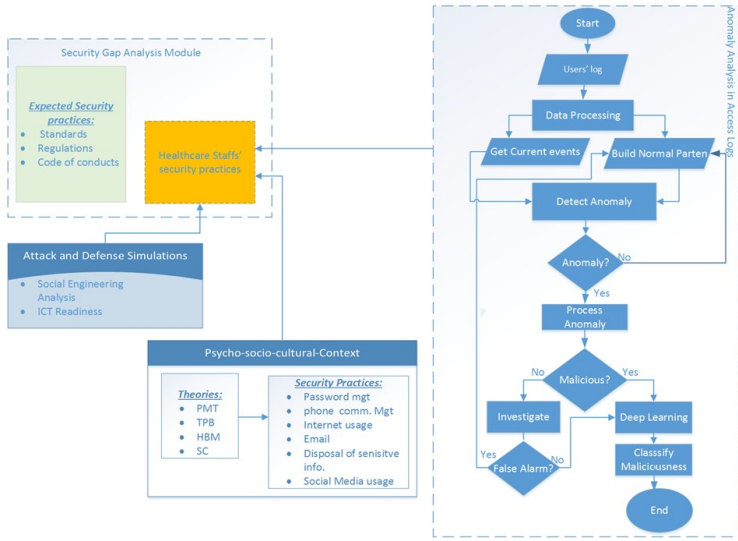


Figure 3.4: HSPAMI designed Framework

tices or behavior. Psycho-socio-cultural attributes can be derived from theories such as social controls (SC), Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB) and the Health Belief Model (HBM). The Security practices, include disposal of sensitive information, social media usage, email usage, password management and other security control related practices in healthcare[4]. The gap of the staffs' security practices in the psycho-socio-cultural aspect is then determined by the variant of their related security practices against the required conducts. The attack and defense simulation module was developed to determine the security resilient of healthcare staffs and the systems against various attacks such as social engineering, ICT readiness for healthcare and denial of service scenarios. The cumulative measure of the security practices of all these models would then be compared with the required security practices of healthcare. The gap is intended to be bridged by using appropriate incentivization methods.

3.5 Discussion

The significant contribution of human factors in healthcare information security is deemed as important as the technical measures. But what is lacking is a comprehensive framework towards mitigating the human elements related threats in the healthcare[19]. The main aim of this paper was therefore to propose a comprehensive framework for modeling and analyzing health-

care staffs' security practices. Prior to this paper, observational measures for profiling healthcare staffs' security practice was formed. Observational measures include observing how healthcare staff respond to the security policies of the institution. The observational measures were formed with regulatory, legal, national and international standards such as the Code of Conduct for Information Security and Data Protection in the healthcare and care services sector of Norway (CCISHCSN), General Data Protection Regulation (GDPR) of European Union (EU), ISO 7799, and other Norwegian Acts and regulations for preserving personal data[4]. One of the purposes of the observational measures was to propose a comprehensive framework which can be used to determine holistic information security metrics from healthcare staffs' information security practices in a broader view. Security metrics of healthcare staffs, obtained through legal, regulations and standards would be reliable to prescribe intervention measures towards achieving their required information security practices. Data breaches in healthcare emanating from the staffs' security practices can be traced in diverse aspects such as psycho-socio-cultural context, healthcare staffs' access logs, attack-defense simulations, organizational factors, training and many more [29]. Due to these wide sources of healthcare staffs' related threats, a holistic approach is required in analysing for the gaps towards mitigating related attacks in healthcare systems. A literature survey was then conducted to serve as input into the development of a framework as shown in Table 12.1 and Figure 12.3. In the survey, frameworks and studies of [3, 6] and [4] only adopted data analysis approach to measure healthcare staffs' security practices. Further, [28, 15] and [14] explored into social engineering methods while [17, 11] and [6] studies concentrated on psycho-socio-cultural context in relation to staffs' security practices [30]. These studies contributed knowledge in mitigating security violations in various aspects but none of them adopted a holistic approach which led to the development of this proposed framework as shown in Figure 12.4.

Concerning access logs, healthcare staffs' practices can be mind in access logs to obtain their unique profiles of the healthcare staffs' practices. Their intentions, desires and goals could also be measured. Mining a combination of such logs for anomalous practices could potentially enhance the efficacy of the detection system [13]. For instance, a malice with the intention of accessing EHR through healthcare facility would have variant physical, network and operating system access profile. Therefore, if there exist significant deviations in all three or four data sources, the probability of the individual being an intruder may be quite high. Also, since healthcare data is very sensitive, an initial assessment in a less sensitive logs for patterns of anomaly and further analyzing the anomalous practice in a more sensitive data could be a privacy conscious care data mining practice. The challenge associated with using only data mining technique includes the point that

Table 3.2: Psychological, Socio-Cultural and Demographic Constructs

Constructs	Definition and Hypothesis
Social Demographics:	Social Demographics relates to staffs' demographics and work related factors that influence healthcare staffs' security practices [27]. Gender, workload, work emergency, role, department and awareness or experience in information security have influence on staff's security practices
Psychological characteristics	Psychosocial characteristics describe the influences of social factors on an individual's mental health and behavior [21]. Perceived severity, susceptibility, barriers, self-efficacy and cues to action, attitude or personality and emotions have influence on healthcare staff's security practices
Social factors	The facts and experiences that influence staffs' information security practices describes social factors. Social Bonding, peer pressure and Trust level impact healthcare staffs' security practices [30, 21]
Cultural Characteristics	The way of life of staffs, such as Environmental norms, cultural beliefs and assumptions have impact on healthcare staff's security practices [30, 21]

if an intruder's security practices does not constitute significant deviations from the legitimate users' profile, the security control measure can be circumvented. Besides, not all scenarios of healthcare security practices can be observed in their activity's logs. For instance, proper disposal of sensitive information, good perceptions relating to information security best practices (such as perceived vulnerability and perceived self-efficacy), frequent data backup, and cautious behavior with suspicious emails [7] and resistance to peer group influence may be challenging to observe in healthcare professionals' log that does not contain such data. Additionally, in modeling and analyzing for security gaps in healthcare staffs' practices, variables such as gender, emergency services, workload and factors which can influence security practices need to be observed. Hypothesis could be formed with the related constructs (as shown in Table 12.2) and statistically assessed. Because, not all these variables require big data related analysis approach or can be tracked in access control related logs of users.

In order to determine the impact of perception variables, the variables which constitute some of the healthcare staffs' traits can be related with the security practices such as password management, disposal of sensitive information and social media usage as shown in Figure 12.6. Perception variables include perceived severity of a threatened event, perceived vulner-

ability, perceived probability of occurrence and self-efficacy as defined in protection motivation theory (PMT). All the psycho-socio-cultural context related frameworks in the literature survey thus [17, 11] and [26] addressed psychological aspect but social and cultural characteristics were lacking in the frameworks. The significance of the user's security practices can be determined with basic statistically surveys in psycho-socio-cultural context, which is effective, easier and less expensive than artificial intelligence methods. Interviews, observations and documents reviews can be adopted with questionnaires in such related studies [30] as shown in Figure 12.1 and Figure 12.6.

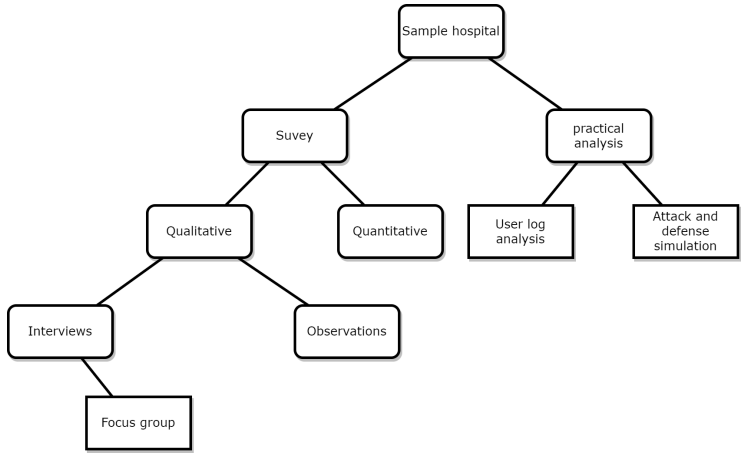


Figure 3.5: Study approach in HSPAMI Framework

In the study of HSPAMI, Yeng et al.,[29] developed observational measures for profiling healthcare staffs' security practices towards mitigating data breaches. The study pointed out some healthcare staffs' security practices which can neither be analyzed with psycho-socio-cultural model nor with the log analysis. In a situation where patients health information (PHI) is being disclosed through the usage of e-mail, text messaging or other unencrypted channels, the right of patients to confidentiality can be violated. In observing for such related vulnerabilities in the context of healthcare staffs' security practices, a method to get PHI and user credentials via social engineering and phishing attacks scenario can be simulated to obtain a metric of how many healthcare staffs are vulnerable to such related attacks for informed decision. Another example is the shutdown of electronic information system scenario (such as virus infection, ransomware and denial of service) which can result in non-availability of essential PHI. Non-availability of essential PHI will result in a range of incorrect patient treatment to loss of lives [16].

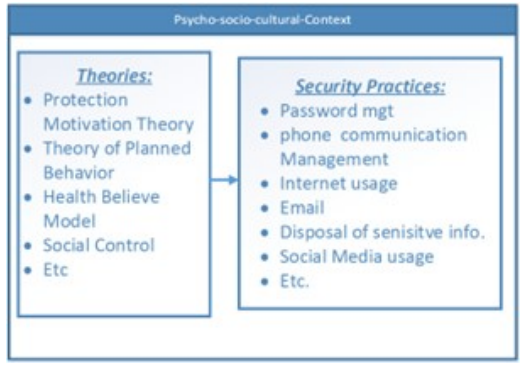


Figure 3.6: Psycho-socio-cultural model

Therefore, testing for the availability of essential PHI in compromised EHR scenarios is deemed most suitable. Further, in an observational measure such as overview of ICT equipment, software, supplier, version numbers, and updates which require monitoring and management, document reviews can be adopted in addition to other possible appropriate measures [29]. In the light of these, psycho-socio-cultural, healthcare staffs' accesses log and simulation of attack-defense modules were adopted in the HSPAMI framework, as a holistic measure to model and analyze the various attack surfaces relating to healthcare staffs' security practices as illustrated in Figure 12.3 and 12.4. The conceptual model was developed with the guide of the observational measures for healthcare security practices which was developed from regulations and legal requirements and standards towards HSPAMI project study. To adopt the proposed HSPAMI framework, a typical healthcare setting would be required to conduct various studies such as practical analysis and survey as shown in Figure 12.5.

The practical analysis would consist of various aspect such as the healthcare staffs access logs and attack and defense simulation. The access logs would include electronic health records access logs, browsing history, operating systems logs or network access logs [29]. Moreover, in the survey studies, integrated approach such as observations, interviews and questionnaires are to be adopted [30]. What is unique and essential about relying on the findings in [29] is the adoption of holistic and tailored approach to obtain the broad spectrum of the observational measures. Additionally, the findings were resulted from a mandated security conducts combined with standards which are most specific to healthcare information security. These standards and code of conducts, are measured up to global standards, legal and regulatory requirement which are being revived to improve upon their effectiveness for healthcare security counter measures [12, 29, 19].

3.6 Conclusion and future works

Following the millions of data breaches which have besieged the healthcare in recent years, HSPAMI project was initiated towards encouraging a security conscious behavior in healthcare staffs. A literature survey was conducted for holistic frameworks that can be used for comprehensive studies for security gaps in healthcare staffs. None of the frameworks in the survey adopted a holistic approach to identify the varying possible entry points in healthcare staffs' security practices. The Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) framework was then proposed. The framework was based on observational measures which was developed from national and international regulations, standards and legal requirements for protecting the privacy right of individuals. HSPAMI-Framework has different modules which can be used to analyze various entry points to obtain security metrics. These metrics can provide guidance for authorities to provide incentivization measures towards building a security conscious care behavior in the healthcare staffs. Incentivization methods that would induce security conscious care practices in healthcare professionals while considering their busy schedule would be explored towards bridging the identified gaps. Aside healthcare, this framework can be adopted in other sectors towards mitigating security issues culminating from human factors.

The HSPAMI framework therefore require empirical evaluation to determine its practical effectiveness before it can be generally adopted for healthcare staffs' security practice related studies. More resources such as time and healthcare staffs availability and privacy preserving methods would be required to be adopted in this study. Since psycho-socio-cultural traits would be related to several staffs' security practices there is a high tendency to have large number of questions in the questionnaire survey. Therefore, proper care should be taken to reduce the number of questions in the questionnaire survey to obtain feasible number of questionnaires for respondents. Appropriate anonymization of access log need to also be taken into consideration to preserve the privacy of the subjects involve in analyzing the logs.

3.7 Bibliography

[1] AJZEN, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of applied social psychology 32*, 4 (2002), 665–683. 100

[2] AJZEN, I., AND MADDEN, T. J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology 22*, 5 (1986), 453–474. 100

[3] BODDY, A., HURST, W., MACKAY, M., AND EL RHALIBI, A. A study into detecting anomalous behaviours within healthcare infrastructures. In *2016 9th International Conference on Developments in eSystems Engineering (DeSE)* (2016), IEEE, pp. 111–117. 100, 101, 102, 103, 107

[4] BODDY, A. J., HURST, W., MACKAY, M., AND EL RHALIBI, A. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 101, 102, 103, 107

[5] CANNOY, S. D., AND SALAM, A. A framework for health care information assurance policy and compliance. *Communications of the ACM 53*, 3 (2010), 126–131. 98, 102

[6] CHEN, Y., NYEMBA, S., ZHANG, W., AND MALIN, B. Specializing network analysis to detect anomalous insider actions. *Security informatics 1*, 1 (2012), 1–24. 100, 101, 102, 103, 107

[7] DAVIS, F. D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly* (1989), 319–340. 108

[8] DOYLE, C., SAMMON, D., AND NEVILLE, K. A design science research (dsr) case study: building an evaluation framework for social media enabled collaborative learning environments (smecles). *Journal of Decision Systems 25*, sup1 (2016), 125–144. 96, 103

[9] DUKE.EDU. Employees' direct deposit rerouted after phishing attack, 2019. Available from: `https://today.duke.edu/2014/01/phishing`. 103

[10] EUGDPR. Key changes with the general data protection regulation, 2019. Available from: `https://eugdpr.org/the-regulation/`. 96

[11] FERNANDEZ-ALEMAN, J. L., SANCHEZ-HENAREJOS, A., TOVAL, A., SANCHEZ-GARCIA, A. B., HERNANDEZ-HERNANDEZ, I., AND FERNANDEZ-LUQUE, L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics 84*, 6 (2015), 454–467. 97, 102, 103, 104, 107, 109

[12] FOR E HEALTH, D. Code of conduct for information security and data protection in the healthcare and care services sector, 2018. Available from: `https://www.enisa.europa.eu/events/NorwegianCodeofconductforinformationsecurityandcloudguidelineEnisa23.11.16`. 95, 98, 99, 105, 110

[13] FOROUGHI, F., AND LUKSCH, P. Observation measures to profile user security behaviour. In *2018 International conference on cyber security and protection of digital services (Cyber Security)* (2018), IEEE, pp. 1–6. 107

[14] GORDON, W. J., WRIGHT, A., AIYAGARI, R., CORBO, L., GLYNN, R. J., KADAKIA, J., KUFAHL, J., MAZZONE, C., NOGA, J., PARKULO, M., ET AL. Assessment of employee susceptibility to phishing attacks at us health care institutions. *JAMA network open 2*, 3 (2019), e190393–e190393. 102, 103, 104, 107

[15] GORDON, W. J., WRIGHT, A., GLYNN, R. J., KADAKIA, J., MAZZONE, C., LEINBACH, E., AND LANDMAN, A. Evaluation of a mandatory phishing training program for high-risk employees at a us healthcare system. *Journal of the American Medical Informatics Association 26*, 6 (2019), 547–552. 103, 104, 107

[16] HARTVIGSEN, G., AND PEDERSEN, S. Lessons learned from 25 years with telemedicine in northern norway, 2015. 95, 102, 109

[17] HUMAIDI, N., AND BALAKRISHNAN, V. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR* (2012), vol. 35, IACSIT Press Singapore, pp. 1–6. 97, 98, 102, 103, 104, 107, 109

[18] HUMER, C., AND FINKLE, J. Your medical record is worth more to hackers than your credit card, 2014. 95

[19] ISO. 27799:2016(en), health informatics information security management in health using iso/iec 27002. 2016., November 2016. 98, 99, 110

[20] LEWIS, B. How to tackle today's it security risks. *ISOfocus 132* (2019), 6–11. 96

[21] MARTIKAINEN, P., BARTLEY, M., AND LAHELMA, E. Psychosocial determinants of health in social epidemiology, 2002. 108

[22] MOFFIT, R. E., AND STEFFEN, B. Health care data breaches: A changing landscape. *Maryland Health Care Commission* (2017), 1–19. 96

[23] OFFERMANN, P., LEVINA, O., SCHÖNHERR, M., AND BUB, U. Outline of a design science research process. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology* (2009), pp. 1–11. 103

[24] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., AND FERGUSON, L. Human factors and information security: individual, culture and security environment. Tech. rep., Defence Science and Technology Organisation Edinburgh (Australia) Command ..., 2010. 99, 100

[25] PATIL, H. K., AND SESHADRI, R. Big data security and privacy issues in healthcare. In *2014 IEEE international congress on big data* (2014), IEEE, pp. 762–765. 96

[26] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 97, 102, 103, 104, 109

[27] SONE, M., MIZUNUMA, K., NAKAJIMA, Y., YASUNAGA, H., AND OHTOMO, K. Job satisfaction, income, workload, workplace, and demographics of japanese radiologists in the 2008 survey. *Japanese journal of radiology 31*, 5 (2013), 364–370. 108

[28] WRIGHT, A., AARON, S., AND BATES, D. W. The big phish: cyberattacks against us healthcare systems, 2016. 101, 102, 103, 104, 107

[29] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 96, 97, 98, 99, 105, 107, 109, 110

[30] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: A literature survey. In *pHealth* (2019), pp. 239–245. 98, 107, 108, 109, 110

Part II

Data-driven approach for analysing security practice

Computer Software and Applications Conference 2019 ;Volum 2. s. 397-404 2019
IEE 43rd Annual Computer Software and Applications Conference (COMPSAC)
https://doi.org/10.1109/COMPSAC.2019.10239

Chapter 4

Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices

Prosper Kandabongee Yeng ; Bian Yang ; Einar Arthur Snekkenes

Abstract

The healthcare sector is characterized with variant situations and services such as emergency services, collaborations in patient care and patient referrals. These activities require erratic accesses and electronic exchange of personal health information (PHI) between health professionals and healthcare organizations. Also, healthcare information is deemed to be among the most confidential of all types of personal data. Analyzing and modeling the security threats emanating from healthcare staffs' security practices therefore need an efficient approach. There is a need for tailored measures to be adopted in assessing healthcare personnel security practices in relation to Confidentiality, Integrity and Availability (CIA) threats. Standards and technical security implementations, required by regulatory bodies, have resulted in tracking healthcare staffs' security practices in various data sources which can be explored for security countermeasures. A literature survey was adopted to obtain the most appropriate observational measures that can be used to empirically study healthcare staffs' security practice analysis, modeling and incentivization (HSPAMI). The survey was conducted in journal and conference articles, healthcare security breaches reports and AI tools for detecting anomalous healthcare staff security practices. The survey results did not find a comprehensive and tailed observational measures suitable for the HSPAMI project. A comprehensive and tailored observational measures were therefore developed from healthcare standards, legal, regulatory aspects, and the code of conduct. Observational measures relating to healthcare security practices such as self-authorization, inter-organizational accesses to PHI and ICT readiness were found to be unique and have not been factored in existing observational measures for efficient profiling of healthcare staffs.

4.1 Introduction

Natural human beings have their basic right to privacy in many parts of the world. The European Union has therefore enacted a General Data Protection Regulation (GDPR) for all European Union and European Economic Area (EU/EEA) member countries to respect this human right to privacy [33]. Norway is bounded to the GDPR through its affiliation to EU [17]. The GDPR of EU has been highly recognized and respected as enshrined in the laws of these member countries [17, 3]. Laws have therefore been promulgated by EU/EEA member countries to implement the GDPR to prevent the abuse of right to privacy of natural persons through the processing of personal data [33]. Personal data relates to data and assessments that can be connected to a natural person [3] and it includes basic identity information such as name, address and ID numbers, Web data such as location, IP address, cookie data and Radio Frequency identification tags, Health and genetic data, Biometric data, Racial or ethnic data, Political opinions and Sexual orientation [17, 3].

In healthcare services, there exists mutual trust and mutual need between healthcare providers and the patients. Much as patients need cure, they require healthcare personnel to be confidential with their disclosed intimate data and information [14]. In the same way, healthcare personnel need and relies on the information and data given by patients to provide effective diagnosis and treatment [14]. This mutual need implies patients to compromise their right to privacy to a limit by sharing their personal information to healthcare personnel with a high trust and condition of confidentiality from the healthcare providers. Healthcare personnel therefore have the responsibility to prevent others from gaining access to or gaining knowledge of information concerning patients' health or medical condition and other personal information known to them in their role as healthcare personnel [14, 27]. Healthcare providers have therefore been mindful to collect only the necessary and relevant patients' data and to be able to keep them as secret as possible to prevent confidentiality breach [14, 9]. However, with the adoption of information Communication Technology (ICT) in healthcare, the confidentiality has been a major challenge. There exists an antagonistic interest between ICT and healthcare provider confidentiality requirement [14]. ICT has muscles for huge data storage, processing and sharing unlimited information while healthcare confidentiality requirement focuses on limiting the spread of information [14]. The evidence is the result of the frequent data breaches in healthcare [16, 15]. Aside the loss of their dignity, the patients suffering may range from fraud to patient injury or death in healthcare related data breaches [9, 21] . Healthcare workers have subtle variant behavior in the usage of ICT systems which can threaten the CIA of the PHI [31]. It has been recorded that, two-thirds of employees have contributed to data breaches [6, 5] through mistakes or deliberate ac-

tions. Technological counter measures such as firewalls, intrusion detection systems, encryption and other security technologies, have been heightened and the adversaries are exploiting the weakest link (humans) in the security chain. The security practices of employees hence need to be strengthened to enhance security in the healthcare [32]. Observational measurement areas in healthcare include but not limited to authorization, authentication, encryption, access control, data or file backups and potential threats to the CIA of the PHI foroughi2018observation14. The specific objectives aimed to seek answers to the following questions; What security measures would be observed and profiled to constitute the necessary and holistic behavioral pattern of each healthcare staff for efficient analysis and modeling? How and where will the security measure be effectively observed? To address these questions, various literatures were surveyed for the common mode of ingress into healthcare systems which are related to healthcare staff practices. Comprehensive data sources and observational measures in which healthcare security practices can be efficiently profiled, were also explored in the survey.

4.2 Methodology and scope

A literature survey was explored as an initial effort to understand the research area under Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) project which is operated by the Centre of Cyber and Information Security of NTNU and funded by the Ministry of Health and Care of Norway. IEEE-Xplore, Google Scholar, Elsevier and Science Direct were searched through for journals and conference papers for observational measures towards profiling healthcare staffs' security practices. The literatures were critically analyzed to be used in the study of HSPAMI. Based on the results, Literatures relating to healthcare data breaches reports, healthcare providers and personnel mandated security practices, standards and best practices were explored. This provided comprehensive view for specifying efficient data sources and observational measures for the efficient profiling of healthcare staff security practices. This was achieved by determining the hypothetical security practices, the alternative hypothetical security practice and the possible security impact of the alternative hypothetical behavior. Possible observational measures were then developed. The study did not include ethical and legal clearance towards the scientific study of personal health information.

4.3 Results

4.3.1 The state-of-the-art

Healthcare staffs' profile consists of a dataset and information which indicate the interaction between the user and a system within a given time [28]. The profiling involves modeling and analyzing their security actions from collected and processed data [22]. So, a comprehensive security actions of healthcare personnel are deemed to be necessary for understanding their goals, habits, interest, preferences, knowledge and skills gaps [11]. So, the data source should be comprehensive to include traces of healthcare security practices of personnel as provisioned in legislatures, regulations and code of conducts [11]. The data gathering should be clear with minimum but necessary and relevant user actions such that the computers or network resources are not impacted [11]. The data should also be gathered to include healthcare staff actions, time and life-cycle to cover all the needed dataset [11]. The healthcare personnel goals, habits, interest, preferences and knowledge often change due to changes in healthcare services such as emergency situations. Therefore, in profiling healthcare security practices, the data gathering need to include all these specific activities in the healthcare services for holistic and efficient results [19]. The healthcare security environment is also deemed to be most critical since it carries a very sensitive and rich information and therefore require much more protection. So, data gathering for profiling staffs' security practices need to take all subtle security practices into consideration [19]. To the best of our knowledge, there has not been such a tailed comprehensive literature survey relating to healthcare security practices. Foroughi et al. analyzed IT security reports and best practices to develop observational measures for cyber security purposes [11]. The knowledge on common causes of security breaches and expected users' IT security behavior were analyzed to profile various IT security observational measures. The source of measures include system setting, installed programs, running processes, online activities, browser history, network connections, warnings, file system and running processes of backup task. Stimulating the observational measures base on user's security practices, provided reliable data sources which can be mined to generate reliable patterns of user behavior [28]. However, Foroughi et al. study did not cover personnel security practices in the healthcare. Personnel behavior is often erratic in healthcare as they strive to provide healthcare in critical situations such as accidents and other emergencies [28]. Therefore, analyzing the security practices of personnel in a mission critical organization would provide a tailed knowledge on the observational measures which can be mined for accurate and efficient patterns of anomalous behaviors.

Additionally, Jason et al. developed a framework for characterizing attacks to detect insider adversaries [25]. The framework has classes of com-

ponents such as attack catalyst, actor, attack and organization characteristics. Attack catalyst consists of events that can have negative impact on staffs or users including demotion. Actor characteristics include potential insider threat such as IT security employee skill set with the potential to attack. Organizational characteristics includes vulnerabilities associated with assets such as networks and servers while attack characteristics deal with behaviors towards attacking a system. These include, for instance, planning and executing logic bomb leading to hacking into company server. After the implementation of the framework, some of the observational measures include inappropriate browsing, accidental leaking sensitive data via email, fraudulent engagement of personnel in logistic company, prison and tax offices respectively. Much as the framework can identify observational measures towards detecting insider-threat from behavioral and technical security practices relating to human factors, the framework faces challenges relating to direct applications to various sectors. For instance, in the healthcare sector, the framework needs to be tuned to accommodate personnel behavior under various services such as emergency services to reduce false alarms. Similarly, Boddy et al. approach to the development of the observational measures was conducted through conceptualization and designing of a framework in healthcare infrastructure [4]. In the framework, input data from computers and medical devices were collected and processed by removing away irrelevant data. The processed data was then stored in a database together with stored known attack behaviors of dataset. This was used to compare with input dataset with the aim to detect malicious intentions. The stored dataset was then processed again and visualized. The output of the visualization could be interfered by the users to set parameters to achieve their situational awareness goals of the infrastructure. An experiment was further conducted with the framework in which an active directory domain controller network statistic (netstat) was captured, analyzed and visualized. The connection type (TCP), source and destination IPs and connection states were captured in the network statistics. Most frequent accesses from foreign IP addresses were realized to be a security threat. The study provided knowledge on how anomalous behavior could be detected by using user behavior visualization technique and also indicated some observational measures such as source and destination IPs. The experiment showed how attackers from external source could be detected but there was no demonstration of how to detect security breaches relating to IP address spoofing or insider attack. Besides, healthcare staffs conduct, involve collaborating on patients care which enables external personnel access. So, using external accesses as a threshold to security threats in the practical demonstration without considering external healthcare personnel legitimate accesses would increase false alarms. This calls for analyzing the entire obligatory conduct of healthcare personnel to determine how their ac-

tivities can be observed for improved security. Boddy et al. did not also indicate how their approach in the framework would not affect system performance since patient input data would always be compared with the known attack patterns.

Walker-Roberts et al. conducted a systematic review of the availability and effectiveness of security solutions to internal threats in healthcare ICT systems [34]. Various methods of security measures including machine learning, profiling and risk control were used. None of the solutions completely counteracted insider threat. Walker-Roberts et al. study did not disclose if healthcare personnel mandated security practices were considered in the development of the security measures. Therefore, there was a limited knowledge on observational measures of the literatures that could be relied on to conduct an empirical study in the healthcare staffs' security practices. However, the study indicated a need for proactive security countermeasures in healthcare which would be considered in this study.

4.3.2 Survy on vendors providing AI solutions in human behavioral security countermeasures in healthcare

In surveying for observational measures and their related data sources in vendors providing AI solutions in human behavioral security countermeasures in healthcare, Sennaar et al., reported on observational variables and their related data sources. According to Sennaar et al.[29], Darktrace system relied on end users and the devices connected to healthcare networks to analyze raw network traffic to uniquely profile the clients' healthcare environment. An acquaintance of the normal security pattern and the associated security tolerance range enables detection of potential threats. Cylance algorithms were fed with data sources from Windows, Mac, and Linux frameworks, consisting of large records of safe and unsafe files and events. Observational variables which are being analyzed include file size, imports, headers and directories which were further aggregated into related clusters in respect to malicious and safe properties.

ClearDATA [29, 30] system mines electronic health records of patients and healthcare personnel records for known security threats. The pattern is then compared with data accesses to determine abnormal accesses. ClearDATA objective was to meet HIPAA compliance across various EHR. Agar's machine learning system intelligence [29, 1, 2] was based on learning about 2 trillion emails per year from email hosting platforms including Yahoo and Google. Features including sender and email type were filtered, analyzed and classified into various categories such as malicious, spam or safe emails for analyzing new emails for maliciousness. Wiretap [29] uses data from various components of healthcare network such as private messages, content files, content from internal and external users of programs such as

Facebook, Slack and Microsoft Office and compared to expected behavior of other healthcare staffs to determine the risk of personnel security practices. Though the various vendors solutions met some observational variables, none of their solutions considered a comprehensive approach towards meeting the CIA of PHI.

4.3.3 Literature survey in healthcare security breaches

The literature survey was extended to healthcare security breaches report for possible observational measures and to provide understanding of trends on common attacks and mode of ingress. The survey found that, in 2018, through the aid of a staff, the health care records of about half the total population of Norway (3 million) were compromised [16]. Also, a phishing attack resulted in breaching 38,000 patients records at Portland, Oregon-based Legacy Health in the United State of America [15]. Personal data such as patients' email accounts, demographic information, dates of birth, health insurance data, billing details, medical data, Social Security numbers and driver's licenses were stolen. In a similar incidence [15], about 1.5 million patient records, including data of the prime minister of Singapore, were breached. A front-end workstation was first compromised to get access to privileged user credentials. In the United States, about 365 breaches were reported in 2018 with hacking being the leading cause of healthcare data breaches followed by unauthorized access and disclosure incidents [20]

4.3.4 Literature survey in Healthcare Staffs' Required Conducts

This section of the study explores efficient methods for determining observational measures of healthcare staffs' practices in literature related to healthcare staffs' mandated conducts, regulations and standards towards the CIA of patients' information. A Comprehensive healthcare staffs' obligated security and confidentiality conduct are spelled out in legal, regulatory, code of conducts, standards and best practices for healthcare organizations and staffs [14]. According to the Norwegian ministry of health and care, the GDPR, the Health Records Act, the Health Personnel Act, the Personal Health Data Filing System Act, the Health Research Act, and the Patients' and Users' Rights Act are deemed most relevant for healthcare data controllers, processors and personnel [14, 7] . These laws, regulations and standards have specified the confidential responsibilities of healthcare staff [27, 21]

As of 25th May 2018, all countries under EU/EEA are being regulated on their personal data privacy and security management. The GDPR outlined rules for protecting natural persons fundamental right to privacy in relation to the processing of personal data and rules relating to personal data movement. Essentially, the GDPR requires businesses and institutions to

protect the personal data and privacy of EU citizens in their dealings within EU/EEA member countries. Failure to comply with this regulation corresponds to a heavy fine [8]. The GDPR was implemented in Norway through the Personal Data Act of Norway, 2018 [3, 10]. The main purpose of the act was for the implementation of the GDPR [3]. The Act ensures that personal data are processed in accordance with fundamental human right to privacy [3].

In the Health Records Act, accesses to patients' records have been improved such that the patient' health records now move along with patients even in referral situations [14, 23]. This helps for the relevant and necessary data to be available for healthcare personnel accesses. The personnel are required to rightly access the patient's data for the provision of quality healthcare while being responsible to confidentiality of the patients' data [14, 23].

The Personal Health Data Filing System Act [26], also exists to provide patients' information and knowledge to public health services and administrations for effective and adequate medical treatment while preserving the patients right to privacy. The Act also support research into patients' data to provide an insight on the state of public health, causes of decreased health and illness. Through research and statistics, the Act contributes toward information on and knowledge of the state of public health. The information and knowledge gained is used for quality assurance, administration, planning and management measures. Much as any person who handles personal health data in relation to [26] has the responsibility of being confidential with patient's personal information, the data controller and processor are responsible to plan with risk assessment measures to have satisfactory security for the CIA of the personal health data.

One of the main objectives of the health personnel act [27] is to ensure trust in health personnel and the health service. Therefore, the health personnel have been constrained with the responsibility to respect patients' personal data confidentiality as specified in chapter 5 of the health personnel Act. The patients act was also enacted to support the respect for human dignity, life and integrity [31] In the reviewed acts [14], there was no technical provisions as how the security measures can be implemented to safe guide CIA of the PHI in healthcare.

The Code of conduct for information security and data protection in the healthcare and care services sector (the code of conduct) [9] was created to facilitate the implementation of adequate technical and organizational measures to meet the CIA requirements for personal data processing. It was developed by the Directorate of e-health in Norway for the implementation of the personal data act in respect to the GDPR [9]. The code of conduct spelled out how the technical and organizational measures are to be implemented to fulfil the personal data privacy requirement and indicated the responsibili-

ties of data controllers, data processors and healthcare personnel in insuring the protection of the personal data.

The code of conduct clearly indicated that, Persons outside the organization or within the organization must not be able to gain unlawful access to personal health information (PHI) and personal data (PD). A summary of the technical implementation requirement includes; Staffs transactions such as, changes, corrections and deletions must be logged in PHI and PA filing systems such as EHR and HR systems. The purpose is to form an audit trail of healthcare security practices. PHI and PD must be accessed by authorized users for only official and therapeutic purpose within the confidentiality arrangement. The technical measures should include self-authorization as an option for authorized users to gain access to PHI and PD without following conventional procedures to access PHI and PD. However, the reason for self-authorization must be documented. For instance, access to PHI and PD filing systems for therapeutic reasons is valid when personnel are officially responsible for a patient who has a planned or completed schedule implementation of measures for the medical treatment. Healthcare personnel's accesses should include their identity, the role to which the authorization has been allocated (if roles are used by the organization), purpose of the authorization and time at which the authorization was given, among others.

Similar provisions were found in other jurisdictions. Health Insurance Portability and Accountability Act (HIPAA) [24] ensures security and privacy of PHI through the HIPAA privacy rule and the HIPAA security rule. HIPAA privacy rule protects personal identifiers, health conditions and payment provision for healthcare. So, appropriate measures and procedures should be kept in place to control abuse of the use and disclosure of PHI. HIPAA security rule protects all personal health information which are created, received, maintained or transmitted in electronic form by the healthcare providers. The rule protects PHI from unauthorized disclosure, integrity and availability of all PHI. The rule also identifies and protect against potential threats to CIA. International Standard Organization (ISO) [19], also provides guidance to healthcare providers and other organizations that possess PHI on the appropriate method to protect CIA of such information. ISO provides unique guidelines on CIA needs of the health sector and its unique operating environments [19]. The ISO 27799 applies ISO/IEC 27002 to the healthcare domain with the appropriate security controls for efficiently protecting personal health information. The ISO 27799 was comprehensively developed with guidelines of personal data protection legislation, obligations, privacy and security best practices, individual and organizational accountability. ISO 27799 aims to protect information such as PHI, pseudonymized data derived from PHI, statistical and research data, including anonymized data derived from PHI.

The Hippocratic oath which is taken by most healthcare personnel, re-

mains very relevant in maintaining CIA of PHI after it was formulated in almost 2500 years ago [21]. In part, healthcare personnel are required to upheld confidentiality with PHI which they might have been aware of due to their official interactions with the patients [21].

In summary, the observational measures which were found in the study includes: Patterns of attempted accesses to PHI, Assessment of trust level of security configurations of computers and networks accessing PHI, Monitoring and controlling social Network accesses in healthcare network, assessing file sharing security, analyzing access identities and analyzing encryption of PHI. Other observational measures include monitoring and controlling, compliance of authorization, access control, authentication, physical accesses of networks, computers and EHR systems, remote communication devices, links and access, backup and recovery management, Audit trails of accesses to computers and peripherals, physical security, networks and EHR, physical security of communications, computer, and display systems and Self-authorization measures.

The data sources which were mostly analyzed for the observational measures of healthcare staff includes system Setting, Installed Programs, running processes, online activities, browser history, network connections logs, warnings, file system and running processes of backup task, social media and email and text messages content analysis and Access Control logs of Electronic Health Records (EHR).

4.4 Discussion

The literature survey was to determine comprehensive observational measures and their related data sources that can be used to empirically study into healthcare staffs' information security practices in HSPAMI project. The impending HSPAMI project results are intended for building a strong security culture towards enhancing the security countermeasures in healthcare. Security countermeasures include diverse aspects such as psycho-socio-cultural context, organizational factors and training. But this study is limited to analyzing and modeling various data sources which are created by healthcare staffs' such as access control logs, network and operating systems logs and other histories of their practices which can be reconstructed to form their unique individual security behavioral profile. The study did not also include ethical and regulatory clearance for researching into personal data.

It is assumed that, the necessary ethical clearance would be obtained prior to researching into personal data. Various literature studies were surveyed for tailored and comprehensive observational measures and their respective data sources that can be explored for healthcare staffs' security countermeasures as summarized in section B, subsection 3 and in Table 1.

Table 4.1: Summary of observational measures for analyzing and modeling healthcare stare security practices

Hypothesis	Possible causes and Related Threats	Detection/Observational Measure	Source
1. Access Control			
There are unauthorized accesses to PHI	User access misconfiguration, impersonations resulting in direct violation of patient' confidentiality, security and privacy issue on necessary and relevant accesses	Compare user access profile with current accesses. Check accesses with authorization register eg purpose, time, location, authorizer, access rights, planned therapeutic patient and schedule, quantum of authorize access,Check misuse of self-authorization and interorganizational accesses	EHR, Network log
Personnel do not have unique authentications Eg password sharing	This can cause unauthorized accesses.	Check for sharing authentication criteria, logins after shift time, and location of logins, login with default password and unique user computer behavior such as keystrokes and mouse clicks dynamics.	EHR
2. Employees, competence and attitude-forming campaigns			
Former employee does not return resources with healthcare data	PHI can be accessed without authorization	Check for dissociated staffs, and assets returned, revoking access right during dissociation such as transfer etc.	EHR
3. Communications Security			
Internet is connected to where PHI is processed	This can provide room for data breaches	Test to ensure internet service is logically separated from areas where PHI is being processed	Network Logs
Not all Healthcare personnel have authorization to use other IT services	The behavior can impact security if websites with trojans and viruses are visited.	Check if user has authorization for email, internet etc., downloaded and installed software. Check if downloads and installations were approved. Check IT services usage with authorization and purpose.	Network logs, browser history, server event logs
PHI is disclosed through the usage of e-mail, text or other unencrypted channels	It compromises the right of patients to confidentiality	Use content filtering to scan email text, images and attachments, for potential threats. Test to get PHI and user credentials via social engineering and phasing attacks	EHR
4. Physical security and the handling of equipment			
Not all personnel obtain keys/access/cards/password through known procedures	Unauthorized persons can have Keys/Access cards to computing resources	Check for abnormal physical access profile of users. Eg. Abnormal physical accesses will deviate from their established profile or pattern	Physical access log
personnel access to data without predefined and preconfigured equipment	Pre-defined equipment helps to identify unknown client computers of a network	Check for user attempted accesses with unregistered endpoint devices, unsuitable, outdated preconfigured devices.	Network,OS, Assets,Updates log
5. Security IT operations			
Healthcare personnel not backing up and testing for prompt recovery of their data, logs and files	Data and Files can get loss when the user computer malfunctions. Without the log, it will be difficult to detect who course a breach	Test backup schedules and recovery, Analyze and test the information system logs and network logs for validity	Backup files
Technical vulnerabilities in equipment are not being managed	Vulnerabilities in equipment's and change management can hinder CIA	Overview of ICT equipment, software, supplier, version numbers, and updates should be monitored and managed. Test for technical vulnerabilities in equipment's, software and change management	ICT equipment and software register change management plan
There is no defined network traffic of personnel accesses	Dictionary, DSS, ransomware and unknown malware [12] attacks	Test for white-listing measure with simulation attack	
6. Digital Communication with healthcare users			
PHI are being sent to patients and to the wrong recipients	There is unauthorized disclosure of PHI	Verify procedures and scan content of information sent to healthcare users	Data handling procedure documents
7. ICT Readiness			
Shutdown of EHR will cause non-availability of essential PHI	Non-available essential PHI will result in a range of incorrect patient treatment to loss of lives	Test for the availability of essential PHI in electronic information shutdown scenarios	
8. Handling of information security breaches			
information security breaches are not being reported	This will prevent, restoring normal system status, eliminating cause of breaches and prevent reoccurrence	Test for reporting information security breaches in a breach scenario	
9. Suppliers and Agreements			
Suppliers, Providers and contractors access do not follow established CIA rules	Adversaries can pose as such and compromise security	Compare accesses with generic normal profiled security practice. Test CIA measures as suppliers, security provider etc.	EHR, Network log

Under section 4.3, subsection 4.3.1, various approaches were used to obtain the observational measures and their related data sources. [11] surveyed literature relating to general security incidence reports and recommended best security practices, by industry players, to compose a security observational measures for insider threats mitigation. Further, [4]and [25] used a conceptualization approach to develop frameworks for observational measures towards insider threat mitigation in healthcare. A systematic review of the availability and effectiveness of security solutions to internal threats in healthcare ICT systems [34] was also explored for observational measures. None of the above studies indicated their observational measures to meet the key security lookups as provisioned in various standards and code of conducts for healthcare security and data privacy protection in Norway [9] as shown in in Table 12.1. The healthcare sector is characterized with variant situations and services such as emergency services and collaborations in patient care which require electronic exchange of personal health information (PHI) between health professionals and healthcare organizations. Also, healthcare information is deemed to be among the most confidential of all types of personal data [19]. Analyzing and modeling the security threats emanating from healthcare staffs' security practices therefore need a holistic, tailored and efficient approach [19]. There is hence a need for tailored measures to be adopted in assessing healthcare personnel security practices in relation to CIA threats in all aspect of the recommended security controls. Standards and regulatory require healthcare organizations to adopt to adequate technical security implementations to be able to proactively detect and mitigate all aspect of the healthcare security issues [9]. This is to reduce risks ranging from unauthorized accesses to denial of services of healthcare electronic information systems [19]. This is to ensure the CIA of the relevant and necessary PHI in healthcare. [11, 25, 4] and [34] studies, covered areas such as access control, physical security, remote access and mobile computing but security measures such as ICT readiness, suppliers and agreements, inter-healthcare-organizational accesses and self-authorizations were not considered [9]. Self-authorization is a technical requirement which is enshrined in the code of conduct for information security and data protection of healthcare in Norway [9]. Self-authorization variable enables healthcare personnel to access individual PHI for therapeutic reasons without following the conventional procedures for PHI access authorization [9]. This is mainly necessary for use in emergency care situation and it is perfectly aligned with the security principle of availability [14, 13]. Though self-authorization is very necessary for patients care, it poses security challenge of blacklisting defenses against inappropriate accesses of PHI since it is susceptible to abuse [9]. Essentially, healthcare staffs' security solutions which lack such tailored observational measures may not be effective since they may impede legitimate PHI accesses, or they may ignore a very big security foot hole for the

advisories [19].

After analyzing healthcare security incidence reports and top AI counter measures for insider threat mitigation, snooping on the medical records, exfiltrating sensitive data to personal accounts, competitors, or bad actors, printing, downloading and exporting patient records and reports, ransomware and phishing attacks were found to be most common [8, 21, 22]. The approaches of the vendor solutions were found to vary from one another but none, employed measures to address all the key security areas which have been provided in the Norwegian code of conduct for healthcare on information security and data protection. This could be due to financial and algorithm computational cost since these AI algorithms gain their intelligence from very large data sources such as emails, endpoint devices and staffs operating practices [29].

Base on the above short comings, a comprehensive and tailored observational measures for profiling, analyzing and modeling healthcare staff security practices were developed in the literature survey. Some of the surveyed literature that were explored include the Code of conduct for information security and data protection for the healthcare in Norway, ISO 27799:2016 and HIPAA security and privacy standards [9, 19]. The observational measures were found to spread across various security measures including access control, employee competence and attitude forming campaigns, communication security, physical security and handling of equipment, security IT operations, digital operations with healthcare users, ICT readiness, handling of information security breaches and suppliers and agreements [9]. All healthcare providers in Norway are to follow details of this spectrum of security controls in the code of conduct to provide efficient technical solutions towards safeguarding the CIA of PHI [9]. The code of conduct was developed by the Norwegian eHealth directorate [9]. Various sources such as the GDPR, Personal Data Act and Healthcare Personnel Act were considered in the development of the code of conduct [9]. The ISO 27799 and the HIPAA security and privacy standards also have similar security measures [24]. The observational measures include self-authorization, interorganizational PHI accesses and ICT readiness as shown in Table **??**.

What is unique and essential about this finding is the holistic and tailored approach which was adopted to obtain the spectrum of the observational measures. Additionally, the findings were resulted from a mandated security conducts combined with standards which are most particular to healthcare information security. Though these standards and code of conducts are not silver bullets, they are measured up to global standards, legal and regulatory requirement which are being revived to improve upon their vitality for healthcare security counter measures [6, 17]. Additionally, under each of the security controls in the code of conduct [9], there are various hypothetical technical implementations which are outlined for users

to adopt. For instance, under access control, technical measures are to be kept in place to prevent unauthorized accesses to PHI. So, the observational measures were developed by forming an alternative hypothesis from the technical security measures. In this instance, the alternative hypothesis was formed as, "There are unauthorized accesses to PHI", as shown in table 12.1. The alternative hypothesis presented a responsibility and a challenge for us to explore and synthesize the observational measures for that alternative hypothesis.

[11, 25, 4], and [34] studies which provided some observational measures were generic and lacked the specific and detailed security attention required in healthcare [9, 19] . For instance, in observing interorganizational accesses of PHI, there is the need to observe for PHI accesses relating to collaborative patient care and accesses by other organizations who have the required permission but not for some therapeutic reasons like collaborative patient care. Additionally, due to the delicate nature of healthcare services, non-availability of a healthcare service could be deemed critical [9]. Critical issues could include life-threatening for patients, organization's operation issues, the incorrect treatment of a patient, loss of efficiency, loss of revenues for the organization and low patient's trust among others [9]. The adoption of the study aim has resulted in similar observational measures which can be observed towards safeguarding the CIA of PHI.

Further to this, how each measure would be observed, were identified to include profiling for machine learning, creating test scenarios and verification of security counter measures for their viability. The profiling of individual security practices towards detecting anomalous practices can be conducted in access control related data such as physical, network and EHR access control related logs [11]. However, it is comparatively complex to adopt to machining learning techniques to determine metrics of healthcare staffs in relation to social engineering activities such as phishing [29]. Therefore, tests scenarios would be deemed most effective [9]. For instance, a supposed phishing email can be sent to healthcare staffs in a controlled environment and the metrics of staffs who pick the bait would be determined. Even if one person is involved would require comprehensive security training and management attention in that regards. Because, the adversaries may require at least, one legitimate user to click the malicious link [18].

Moreover, various data sources were identified alongside with the observational measures. These include logs from EHR, Network, browser history, physical security access logs and OS as shown in Table 1. Mining a combination of these logs for anomalous practices could potentially enhance the efficacy of the detection system [11]. For instance, an advisory who want to access EHR through healthcare facility would have variant physical, network and operating system access profile. Therefore, if there exist deviations in all three or four data sources, the probability of the individual being

an intruder would be quite high. But in observing such measures, effective and efficient training of the algorithms are required in order not to prevent legitimate healthcare personnel from accessing systems for therapeutic reasons.

4.5 Limitations, conclusion and future works

Healthcare PHI is deemed to be one of the most sensitive personal data which its CIA require enhanced security controls. The richness of the PHI has attracted malice despite the technological security countermeasures. The advances of the adversary for PHI has the tendency of impacting CIA, ranging from fraud to loss of life. This has motivated a HSPAMI study which stands to study into healthcare staffs' security practices towards building a security conscious care behavior through incentivization. A literature survey was then conducted in this regard to explore for comprehensive and tailed security observational measures which can be used to analyse and model to detect anomalous behaviors. Literature relating to healthcare security breaches report, some top AI systems for healthcare insider threat detection, standards, regulations and legislation's, code of conducts and other literature relating to observational measures were surveyed. Comprehensive and tailed security observational measures such as self-authorization, interorganizational accesses of PHI and ICT readiness were identified to be some of the most essential observational variables. Machining learning technique can be used to analyze and model the observational measures to profile individual staffs' security practices for anomalous tracking. Test scenarios can also be developed from the results to test for social engineering related behaviors of healthcare staffs. The study results can also be used to test for ICT readiness by testing scenarios to determine if the necessary and relevant PHI would be available in situations where the electronic health records is deemed not available.

The observational measured identified are deemed to be of high level and would require more detailed requirement analysis prior to implementation. A second expert opinion would also be required to assess these variable before they are used for empirical study.

4.6 Bibliography

[1] AGARIINC. Advanced threat protection solutions—agari email protection, July 2019. Available from: `https://www.agari.com/products/advanced-threat-protection/`. 122

[2] AYYAGARI, R. An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security 8*, 2 (2012), 33–56. 122

[3] BEREDSKAPSDEPARTEMENTET. Proposition 56 ls (2017–2018)/act on the processing of personal data (the personal data act). 2018, regjeringen.no., April 2019. Available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/norway. 118, 124

[4] BODDY, A., HURST, W., MACKAY, M., AND EL RHALIBI, A. A study into detecting anomalous behaviours within healthcare infrastructures. In *2016 9th International Conference on Developments in eSystems Engineering (DeSE)* (2016), IEEE, pp. 111–117. 121, 128, 130

[5] CISCO. Cisco 2017 annual cybersecurity report: Chief security officers reveal true cost of breaches and the actions organizations are taking, April 2017. Available from: http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna. 118

[6] CNN.COM. A convicted hacker debunks some myths,, April 2005. Available from: http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna. 118

[7] DIABETESDAGBOKA. Norwegian centre for e-health research, July 2019. Available from: http://www.diabetesdagboka.no/en. 123

[8] EUR-LEX. The european parliament and the council of the european union, regulation (eu) 2016/679, eu, editor, July 2016. Available from: https://lovdata.no/dokument/NL/lov/2014-06-20-42. 124

[9] FOR EHEALTH, D. Code of conduct for information security and data protection in the healthcare and care services sector, April 2019. Available from: https://www.ehelse.no/normen/documents-in-english. 118, 124, 128, 129, 130

[10] FOR EHEALTH, D. Implementation of gdpr in health care sector in norway, July 2019. Available from: https://ehelse.no/personvern-og-informasjonssikkerhet/eus-personvernforordning/implementation-of-gdpr-in-health-care-sector-in-norway. 124

[11] FOROUGHI, F., AND LUKSCH, P. Observation measures to profile user security behaviour. In *2018 International conference on cyber security and protection of digital services (Cyber Security)* (2018), IEEE, pp. 1–6. 120, 128, 130

[12] GDPR. Report, businesses at risk due to unidentified network traffic according to global survey - gdpr.report., October 2018. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/&attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf. 127

[13] GOODRICH, M., AND TAMASSIA, R. *Introduction to Computer Security: Pearson New International Edition PDF eBook*. Pearson Higher Ed, 2013. 128

[14] HARTVIGSEN, G., AND PEDERSEN, S. Lessons learned from 20 years with telemedicine in north norway. *Forthcoming lecture book, Norwegian Centre for Integrated Care and Telemedicine 370* (2012). 118, 123, 124, 128

[15] HEALTHCAREITNEWS. Healthcare it news, April 2019. Available from: https://www.healthcareitnews.com/. 118, 123

[16] HUGHES, O. Norway healthcare cyber-attack 'could be biggest of its kind', April 2019. Available from: https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/. 118, 123

[17] ICLG. International comparative legal guides. 2019, April 2019. Available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/norway. 118

[18] ISLAM, R., AND ABAWAJY, J. A multi-tier phishing detection and filtering approach. *Journal of Network and Computer Applications 36*, 1 (2013), 324–335. 130

[19] ISO. Iso 27799:2016(en), health informatics information security management in health using iso/iec 27002, April 2017. Available from: https://www.iso.org/standard/62777.html. 120, 125, 128, 129, 130

[20] JURNAL., H. Hipaa journal, healthcare data breach statistics., July 2019. Available from: https://www.hipaajournal.com/healthcare-data-breach-statistics/. 123

[21] KANTARJIAN, H., AND STEENSMA, D. P. Relevance of the hippocratic oath in the 21st century. *The ASCO Post 5*, 16 (2014). 118, 123, 126

[22] KUSSUL, N., AND SKAKUN, S. Intelligent system for users' activity monitoring in computer networks. In *2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (2005), IEEE, pp. 306–309. 120

[23] LOVDATA. Implementation of gdpr in health care sector in norway, July 2019. Available from: https://lovdata.no/dokument/NL/lov/2014-06-20-42. 124

[24] NEUHAUS, C., POLZE, A., AND CHOWDHURYY, M. M. *Survey on healthcare IT systems: standards, regulations and security*. No. 45. Universitätsverlag Potsdam, 2011. 125, 129

[25] NURSE, J. R., BUCKLEY, O., LEGG, P. A., GOLDSMITH, M., CREESE, S., WRIGHT, G. R., AND WHITTY, M. Understanding insider threat: A framework for characterising attacks. In *2014 IEEE security and privacy workshops* (2014), IEEE, pp. 214–228. 120, 128, 130

[26] OMSORGSDEPARTEMENTET. Personal health data filing systems and the processing of personal health data (personal health data filing system act), in 042041-990016. 2006, regjeringen.no, October 2006. Available from: https://www.datatilsynet.no/globalassets/global/english/personal_health_data_filing_system_act_20100907.pdf. 124

[27] OMSORGSDEPARTEMENTET. Act of 2 july 1999 no. 64 relating to health personnel etc., April 2019. Available from: https://www.regjeringen.no/no/dokumenter/act-of-2-july-1999-no-64-relating-to-hea/id107079/. 118, 123, 124

[28] OUAFTOUH, S., ZELLOU, A., AND IDRI, A. User profile model: A user dimension based classification. In *2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA)* (2015), IEEE, pp. 1–5. 120

[29] SENNAAR, K. Cybersecurity in healthcare, comparing 5 ai-based vendor offerings, June 2019. Available from: https://emerj.com/ai-application-comparisons/cybersecurity-healthcare-comparing-5-ai-based-vendor-offerings/. 122, 129, 130

[30] SENNAAR, K. Cybersecurity in healthcare – comparing 5 ai-based vendor offerings, June 2019. Available from: https://emerj.com/ai-application-comparisons/cybersecurity-healthcare-comparing-5-ai-based-vendor-offerings/. 122

[31] SHILTON, K., SUBRAMANIAM, M., VITAK, J., AND WINTER, S. Qualitative approaches to cybersecurity research. *IConference 2016 Proceedings* (2016). 118

[32] [TETZ, E. Network firewalls: Perimeter defense - dummies, April 2017. Available from: https://www.dummies.com/programming/networking/cisco/network-firewalls-perimeter-defense/.. 119

[33] UNION, E. The european parliament and the council of the european union, regulation (eu) 2016/679 of the european parliament and of the council, in 95/46/ec, 2016 official journal of the european union, April 2019. Available from: https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1. 118

[34] WALKER-ROBERTS, S., HAMMOUDEH, M., AND DEHGHANTANHA, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access 6* (2018), 25167–25177. 122, 128, 130

Advances in Intelligent Systems and Computing 2020 ;Volum 1250.
https://doi.org/10.1007/978-3-030-55180-3_1

Chapter 5

Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review

Prosper K. Yeng, Livinus N. Obiora, Ashenafi Zebene Woldaregay, Bian Yang and Ennar Snekkenes

Abstract

Data breaches in healthcare continue to grow exponentially, calling for a rethinking into better approaches of security measures towards mitigating the menace. Traditional approaches including technological measures, have significantly contributed to mitigating data breaches but what is lacking is the development of the "human firewall," which is the conscious care security practices of the insiders. As a result, the healthcare security practice analysis, modeling and incentivization project (HSPAMI) is analyzing healthcare staffs' security practices in various scenarios including big data. The intention is to determine the gap between staffs' security practices and required security practices for incentivization measures. To address the state-of-the art, a systematic review was conducted to pinpoint appropriate AI methods and data sources that can be used for effective studies. Out of about 130 articles, which were initially identified in the context of human-generated healthcare data for security measures in healthcare, 15 articles were found to meet the inclusion and exclusion criteria. A thorough assessment and analysis of the included article reveals that, KNN, Bayesian Network and Decision Trees (C4.5) algorithms were mostly applied on Electronic Health Records (EHR) Logs and Network logs with varying input features of healthcare staffs' security practices. What was found challenging is the performance scores of these algorithms which were not sufficiently outlined in the existing studies.

5.1 Introduction

The enormous increase in data breaches within healthcare is frightening and has become a source of worry for many stakeholders such as healthcare providers, patients, national and international bodies. In 2018, the healthcare sector recorded about 15 million records which were compromised in about 503 data breaches [36, 22]. This was a triple of 2017 data breaches in healthcare. In the middle of 2019, the number of compromised records in healthcare were more than 25 million, implying that by the end of 2019, the number of compromised records might be sky rocketed [22]. Greater proportion of the breaches (59%) were perpetrated by insiders [36] who are authenticated users of the systems [43]. Most of the adversaries were motivated by financial gains (83%) and other motives such as convenience (3%), grudges (3%), industrial espionage (2%) [36]. The number of data breaches in healthcare has substantially exceeded that of the financial sector and almost caught up with other public sector entities [36]. The tremendous increase in data breaches in recent time within healthcare, have therefore left many to ponder about the possible causes. The healthcare data is comparatively richer and has become "honey-port", attracting the malice [23, 24]. Health data has vast scientific, societal, and commercial values, which cause cyberattacks and black market targeting of this data. Healthcare data can be used to commit multiple dark activities in the dark web as detection of breaches, related updates and correction of the compromised data takes a longer time. Another angle of thought is that, the healthcare personnel are busy with their core healthcare duties and are less experienced in information security conscious care behavior. This leaves room for adversarial attacks. The technological measures (such as firewall, intrusion detection or prevention systems, antiviruses and security governance configurations) have been strengthen [14] and making it difficult for external cyber criminals to inappropriately access data [1, 29]. But there is no related development of "the human firewall" [9]. The human firewall is the information security conscious care behavior of the insiders [9, 32]. The human firewall has not gained equal attention, and this is vulnerability which the cybercriminals tend to exploit for easy entry [42]. By virtue of their access privileges, healthcare insiders are "double-edged sword". While their privileges enable them to provide therapeutic care to patients, healthcare staffs' errors and deliberate actions can compromise the Confidentiality, Integrity and Availability (CIA) of healthcare data. Additionally, external malice can masquerade insiders to compromise healthcare data through various ways, including social engineering methods [43]. Furthermore, the healthcare environment is relatively complex and delicate, making it hard for healthcare information security professionals to design stricter access control policies. So, access control mechanisms in healthcare are mostly designed with a degree of flexibility to enable efficient patient management. While such de-

sign considerations are very important and meets the availability attribute of the CIA, the healthcare systems remain vulnerable. The broad range of access flexibility can be abused by the insiders. This can also be a dream for cyber criminals to adopt various diabolic means of gaining insiders credentials to enable them to equally have larger access. The incidence of data breaches could bring various consequences including denial of service for timely medical services, negative impact on mutual thrust between patient and healthcare providers, breaches to individual's privacy and huge finds to healthcare providers by national and international regulatory bodies.

The general objective of this study was to therefore to identify, assess, and analyze the state-of-the-art Artificial Intelligence strategies and their hybrid aspect which can be used to efficiently detect anomaly and malicious events in healthcare staff's security practices in their access related data towards improving counter-measures for healthcare staffs related security breaches. Specific objectives include;

- Identifying AI learning algorithms which can be used to efficiently profile healthcare staff security practices, for anomalies detection.
- A ssess and analyzed the design considerations of the methods (such as the tolerance ranges or thresholding mechanisms provided to accommodate non-treacherous user behaviors i.e., new users, mistakes and during emergencies) towards mitigating false positives.
- Assess and analyze their performance metrics and other suitable evaluation methods
- Determine associated challenges in the usage of the algorithms and how these challenges can possibly be overcome.

5.1.1 Motivation, Scope and Problem Specification

Healthcare Security Practice Analysis, Modelling and Incentivization (HSPAMI), is an ongoing research project in which an aspect involves modelling and analyzing data with AI methods to determine the security practices of healthcare staffs, towards improving their security conscious care behavior. In analyzing healthcare related data, there is the need to consider details of the methods and data sources in view of the unique and critical nature of the sector. In a related study, Walker-Roberts et al., conducted a systematic review of "the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure" [39]. Among various teams few machine learning methods were identified to be used for intrusion detections and preventions. The methods that were identified are Petri net, Fuzzy logic, K-NN, K-Decision tree(RADISH system) [39, 8, 17] and inductive machine

learning methods [39, 8, 17, 13]. In a similar way, Islam et al conducted a systematic review on data mining for healthcare analytics [25]. Categories such as healthcare sub-areas, data mining techniques, type of analytics, data and data sources were considered in the study. Most of the data analysis were for clinical and administrative decision making. The data sources were mostly human generated from electronic health records. Other studies which explored for related methods includes [20] and [19].

Even though, the studies [39, 25] were in healthcare context, details of the algorithms and data sources were not considered. For instance, the features of the data sources and algorithm performance methods, were not deeply assessed in their studies. Additionally, the studies of [20]and [19] were general and not healthcare specific. So unique challenges within healthcare environment were not considered in their study. To this end, the study aimed to explore into details, AI methods and data sources in healthcare that can be efficiently used for modeling and analyzing healthcare professionals' behavior. Healthcare professionals and healthcare staffs were used interchangeably in this study to include but not limited to nurses, physicians, laboratory staff and pharmacies who access patients records for therapeutic reasons.

5.2 Background

Security practice of healthcare staffs includes how healthcare professionals respond to the security controls and measures towards achieving the CIA goals of the healthcare organizations.

Healthcare professionals are required to conduct their work activities in a security conscious manner to maintain the CIA of healthcare environment. For instance, borrowing of access credentials could jeopardize the purpose of access control for authorized users and legitimate accesses. Additionally, the inability to understand social engineering scammers' behavior can lead to healthcare data breaches.

Various ways can be adopted to observe, model and analyze healthcare professionals' security practices. Perception and socio-cultural context can be adopted by analyzing the healthcare staffs' security perception, social, cultural and socio-demographic characteristics with their required security practices. Also, Attack-Defense simulation can be used to measure how healthcare staffs understand social engineering related tricks. Furthermore, data-driven approach with artificial intelligence (AI) methods could be adopted to understand the security risk of each healthcare professions. The findings can then help decision makers to introduce appropriate incentive methods and solve issues which are hindering sound information security practice towards enhancing conscious care behavior. But this study is focused on exploring for appropriate AI methods and data sources that

can be used to modeled and analyzed healthcare security practices. Therefore, psycho-socio-cultural context and attack-defense simulations are beyond the scope of this paper.

5.2.1 Data-Driven and Artificial Intelligence in healthcare security practice analysis

Advances in computational and data sciences along with engineering innovations in medical devices have prompted the need for the application of AI in the healthcare sector [33]. This has the potential of improving care delivery and revolutionizing the healthcare industry. AI can be referred to as the use of complex algorithms and software to imitate human cognitive functions[26]. It involves the application of computer algorithms in the process of extracting meaning from complicated data and to make intelligent decisions without direct human input. AI is increasingly impacting every aspects of our lives and the healthcare sector is not an exception. In recent years, the healthcare sector is experiencing massive deployments of AI in the bid to improve the overall healthcare delivery. There is currently no consensus on the classification of the applications of AI in healthcare. However, we rely on the classification of the application of AI in healthcare described in [38] to briefly discuss deployment of AI in healthcare.

The deployment of AI in healthcare sector has been classified in [38] to include; expert systems, machine learning, natural language processing, automated planning and scheduling, and image and signal processing. Expert systems are AI programs that have been trained with real cases to execute complicated tasks [37]. Machine learning employs algorithms to identify patterns in data and learn from them and its applications can be grouped into three, namely; supervised learning, unsupervised learning, and reinforcement learning [38]. Natural language processing facilitates the use of AI to determine the meaning of a text by using algorithm to identify key words and phrases in natural language [38]. For automated planning and scheduling, it is an emerging field in the use of AI in healthcare that is concerned with the organization and prioritization of the necessary activities in order to obtain desired aim [38]. And image and signal processing involve the use of AI to train information extracted from a physical occurrence (images and signals) [38].

The common characteristics of all these applications is the utilization of massive data that is being generated in the healthcare sector to make better informed decisions. For instance, the collection of healthcare staffs' generated data, has been used for disease surveillance, decision support systems, detecting fraud and enhancing privacy and security [10]. In fact, the code of conduct for healthcare sector of Norway require the appropriate storage and protection of access logs of healthcare information systems for secu-

rity reasons [16]. The healthcare staffs' accesses within the network or electronic health records (EHR), leaves traces of their activities which can be logged and reconstructed to form their unique profiles [16]. The healthcare staffs' accesses within the network or electronic health records (EHR), leaves traces of their activities which can be logged and reconstructed to form their unique profiles [41]. So, the appropriate AI methods can then be used to mine in such logs to determine the unique security practices of the healthcare staffs. Such findings can support management to adopt to the suitable incentivization methods towards improving on the security conscious care behavior in healthcare. Therefore, this study stands to explore for the appropriate AI methods and data sources that can be used to observe, model and analyzed the security practices of healthcare staffs.

5.3 Method

The objective of this study was to identify, asses and analyze the state-of-the-art data-driven and artificial intelligence (AI) algorithms along with their design strategies, and challenges. The study is towards analyzing healthcare professionals' security practices in the context of big data or human generated data in Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) project. A literature search was conducted between June 2019 and December 2019 through Google Scholar Science Direct and Elsevier, IEEE Explore, ACM Digital. Different key words such as "Healthcare", "staff", "employee", "Information security", "behavior", "Practice", "Threat", "Anomaly detection", "Intrusion detection", "Artificial Intelligence" and "Machine Learning ", were used. For a good quality searching approach, the key words were combined using Boolean functions of 'AND', 'OR' and 'NOT'. Peer reviewed journals and articles were considered. The inclusions and exclusions criteria were developed based on the objective of the study and through rigorous discussions among the authors. Basic selection was done by initially skimming through the titles, abstracts and keywords to retrieve records which were in line with the inclusion and exclusion criteria. Duplicates were filtered out and articles, which seems relevant, based on the inclusion and exclusion criteria, were fully read and evaluated. Other appropriate articles were also retrieved using the reference list of accepted literatures. Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) flow diagram was used to report the article selection and screening [30].

5.3.1 Inclusion and Exclusion Criteria

For an article to be included in the review, the study has to be an anomaly detection or intrusion detection in healthcare using artificial intelligence meth-

Prefix	Description
CH	Main text body labels
FIG	Figures and illustrations
EQ	Equations
TAB	Tables
ALG	Algorithms
DEF	Definitions
THE	Theorems, corollaries, propositions, and lemmata

Table 5.1: Cross-reference label prefix format

ods in healthcare professionals' generated access logs data or patterns. Any other article outside the above stated scope (such as articles in medical cyber-physical devices, body area networks etc.) including literatures in other languages, except English, were excluded.

5.3.2 Data Collection and Categorization

The data collection and categorization were developed based on the objective and through literature reviews and authors discussions. The categories have been defined exclusively to assess, analyzed and evaluate the study as follows:

- Type of AI method: This category includes explicit machine learning methods such as, Support Vector Machine (SVM), Bayesian network, etc.
- Type of Input: This category includes the features which were used by the algorithm. This could include access location, time, log in failed attempts etc.
- Input Sources: This attribute refers to the kind of access logs data, which was used in the study. Such sources include browser history, network logs, host-based activity logs and electronic health records logs
- Data Format, Type, Size, and Data Source: This category could include file format such as XML, CSV
- Input Preprocessing: Defines how the data was preprocessed from unstructured to structured, and how missing and corrupted input data were handled.
- Application Scenario: This category defines the context of which the algorithm was implemented such as intrusion or anomaly detection.

- Ground Truth: Refers to the kind of training set used in training the model.
- Privacy approach: This defines the privacy method used to safeguard the privacy right of individuals who contributed to the data source.
- Performance Metrics or Evaluation Criteria: This includes the measures used to assess the accuracy of the study. It includes metrics such as specificity, sensitivity, receiver operating characteristic (ROC) curves, and others
- Nature of Data Sources: This category specifies if the data used was synthetic or real data.

5.3.3 Literature Evaluation and Analysis

The selected articles were assessed, analyzed and evaluated, based on the above defined categories. The analysis was performed on each of the categories (Type of AI method, type of input, input source, preprocessing, learning techniques, performance methods etc.) to evaluate the state-of-the-art approaches. Percentages of the attributes of the categories were calculated based on the total number of counts (n) of each type of the attribute. Some studies used multiple categories, therefore, the number of counts of these categories exceeded the total number of articles of these systems presented in the study.

5.4 Results

After searching in the various online databases, a total of 130 records were initially identified by following the guidelines of the inclusion and exclusion criteria in the reading of titles, abstracts, and keywords. A further assessment of these articles through skimming of the objective, method and conclusion sections led to a further exclusion of 77 articles which did not meet the defined inclusion criteria. After removing duplicates, 42 articles were fully read and judged. After the full text reading, a total of 15 articles were included in the study and analysis as shown in the Figure 5.1. As shown in the Figure **??**, the topic of data-driven and AI for analyzing healthcare security practice has seen consistent interest.

As shown in Figure 5.2, most of the literature were identified in google scholar and followed by IEEE Explore and ACM Digital Library.

The articles were published between 2010 and 2019 as shown in Figure 5.3

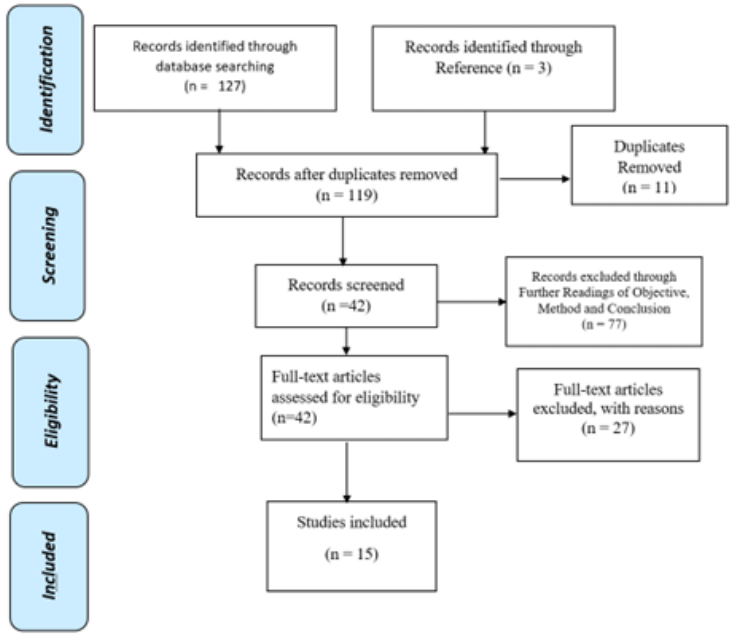


Figure 5.1: Flowchart of the systematic review process

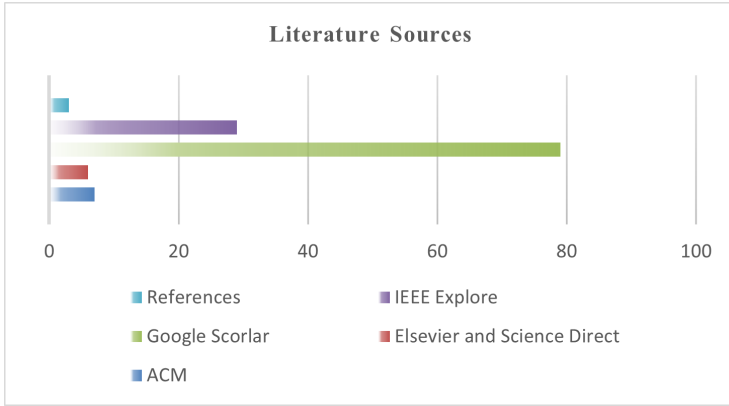


Figure 5.2: Literature Sources

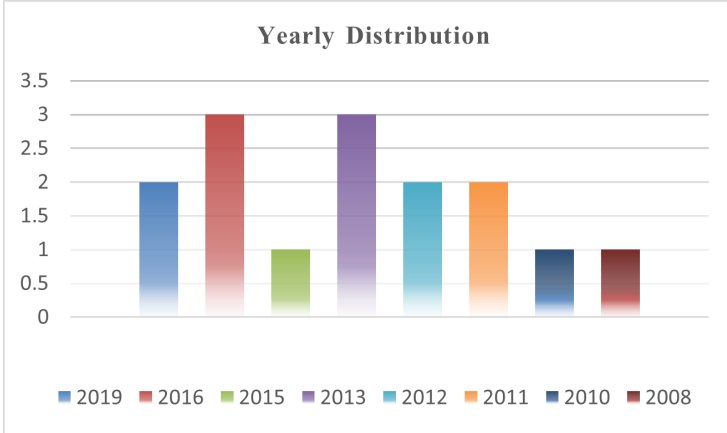


Figure 5.3: Yearly Distribution

5.4.1 Evaluation and Analysis

Evaluation and analysis of the articles were carried out as described above, and the main finds are presented below.

Articles in the Study: The articles and their related categorizations, such as algorithms, features and data sources are shown in Table 12.1.

5.4.1.1 Algorithms

The algorithms which were found in the review are as shown in Table 5.3. KNN method was mostly used (17%), followed by Bayesian Network (14%) and C4.5 decision tree (10%).

5.4.1.2 Features

With reference to Table 5.4, the features which were mostly used include Users ID (19%), Date and Time attribute (17%), Patient ID (16%) and Device Identification (DID)(14%).

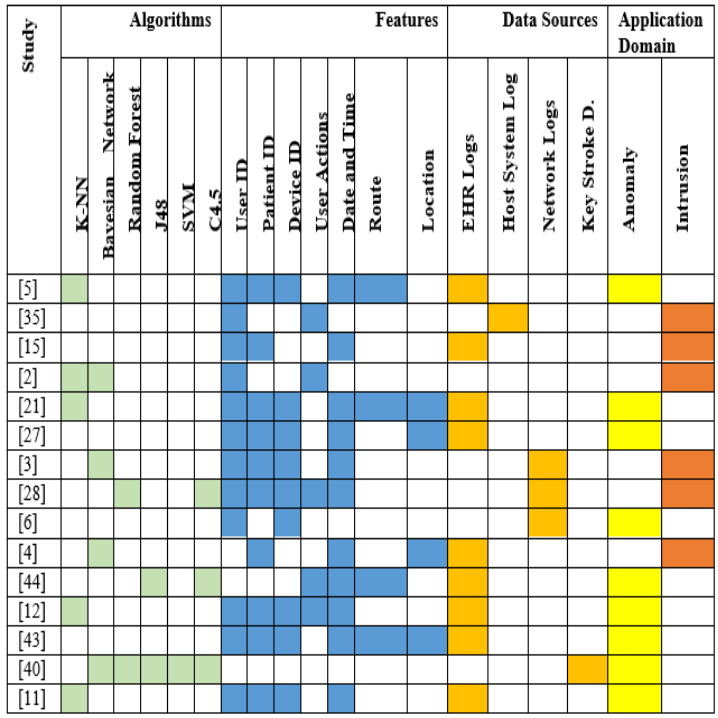
5.4.1.3 Data sources

Most of the data sources were EHR logs (60%) and Network logs (20%) as shown in Table 5.5.

5.4.1.4 Performance methods

Regarding performance methods as shown in Table 5.6, FP (23%), TP (20) % and Recall (13%) were mostly used to assess the studies.

Table 5.2: Algorithms, Features, their related Data Sources and application domain



5.4.1.5 Application scenario

The studies in the review were mostly applied for anomaly detection (60%) and Intrusion detection (40%) as shown in Figure 5.4.

5.4.1.6 Data format

Regarding file format, Comma separated values (CSV) was commonly used as the file format [7, 35]. Some studies also used SQL file format [4, 15].

5.4.1.7 Ground Truth

In the review, the ground truth was being established with similarity measures, observed and controlled practices and historical data of staffs' practices as shown in Table 5.7.

Table 5.3: Algorithms and their respective proportions

Algorithm	Count	%
K-Nearest Neighbors (KNN) [5, 2, 21, 12, 11]	5	17
Bayesian Network (BN) [6, 2, 3, 40]	4	14
C4.5 [28, 44, 40]	3	10
Random Forest [28, 40][34, 39]	2	7
J48[44, 40][37, 39]	2	7
Principal Component Analysis(PCA) [11][40]	2	7
e Spectral Project Model[11][40]	1	3
SVM [40][39]	1	3
k-Means[35][28]	1	3
Spectral Project Method	1	3
Ensemble averaging and a human-in-the-loop model [6] [35]	1	3
Partitioning Around Medoids with k estimation (PAMK)[28] [34]	1	3
Distance Based Model [27]	1	3
White-box anomaly detection system [15]	1	3
C5.0	1	3
Hidden Markov Model (HMM) [3]	1	3
Graph-Based[43]	1	3

Table 5.4: Features used

Feature	Count	%
User Identification (UID)	12	19
Patient Identification (PID)	10	16
Device ID(DID)	9	14
Access Control (AC)	5	8
Date and Time	11	17
Location	4	6
Service/Route	5	8
Actions (Delete, Update, Insert, Copy, View)	3	5
Roles	3	5
Reasons	1	2

5.4.1.8 Privacy preserving data mining approach

Privacy preserving methods which were adopted in study are tokenization [7] [6], deidentification [21] and removal of medical information [44].

5.4.1.9 Nature of data sources

With reference to Figure 5.5, the nature of the data sources which were used in the studies were mostly Real data (80%) and synthetic data (20%).

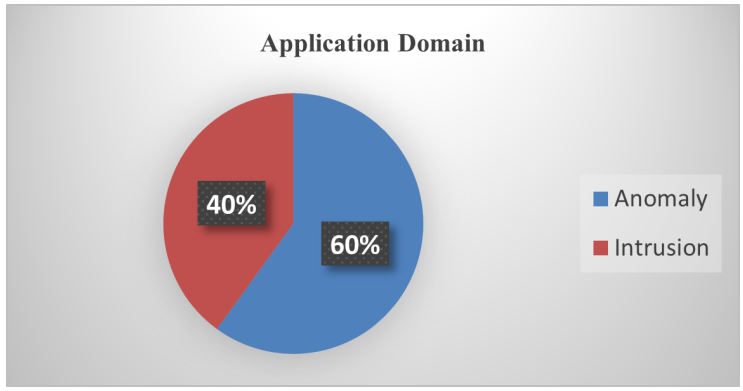


Figure 5.4: Application domain

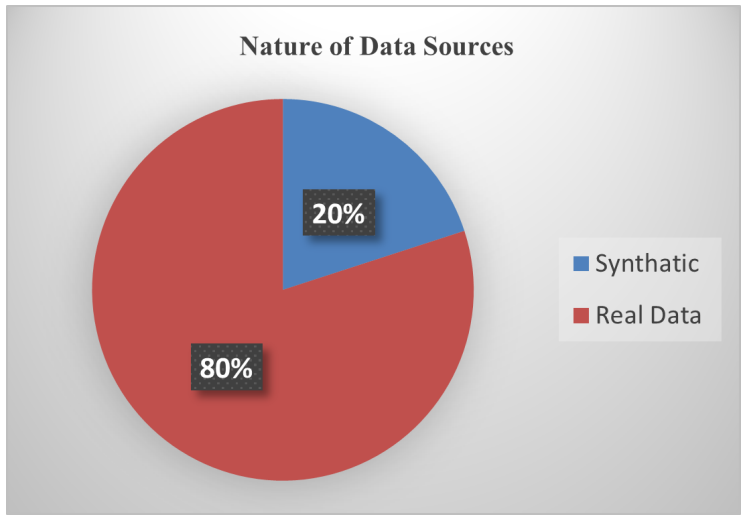


Figure 5.5: Nature of data sources

Table 5.5: Data Sources Used

Data Source	Count	%
Electronic Health Records logs (EMR) Logs	9	60
Host-Based Logs	1	7
Network Logs	3	20
Key-Stroke Activities	1	7

Table 5.6: Performance Methods

Performance Methods	Count	%
True Positive (TP)	8	20
False Positive (FP)	9	23
False Negative (FN)	5	13
Receiver Operating Characteristic ROC Curve	5	13
Area Under ROC (AUC) curve	3	8
Recall (Sensitivity)	5	13
Precision	3	8
Accuracy	2	5

Table 5.7: Ground Truth

Ground Truth	Count	%
Similarity Measures	3	38
Observed practices	3	38
Historical data	2	25

5.5 Discussion

The main purpose of this systematic review was to find details of Artificial Intelligence (AI) methods and suitable healthcare staffs' generated security practice data, that can be efficiently mined to determine the status of healthcare security practices with respect to required security practices. The main findings in the study are as shown in Table 5.8. With reference to Figure **??**, and Table 12.1, there were 15 studies which met the inclusion and exclusion criteria. Recently, a related systematic review for countermeasures against internal threats in healthcare also found about 5 machine learning methods, [**?**] which were fit for such measures. This suggests that the adoption of AI methods for modeling and analyzing healthcare professionals' generated security practice data, is still an emerging topic of academic interest.

5.5.1 AI methods

As shown in Table 5.3 and Table 5.8, various algorithms were identified in the study, but the most used methods were KNN and BN algorithms. K-

Table 5.8: Principal findings

Category	Most Used
Algorithms	KNN and Bayesian Networks
Features	User IDS, Patient IDs, Device ID, Date and Time, Location,
Data sources	Route and Actions
Application Domain	Electronic health Records (EHR) logs and Network logs
Performance Methods	Anomaly Detection
Data Format	True Positive, False Positive, False Negative, ROC curve, AUC
Nature of Data Sources	CSV
Ground Truth	Real Data logs
Privacy preserving approaches	Similarity measures and observed data
	Tokenization and deidentification

Nearest Neighbors (kNN) is a supervised learning -based classification algorithm [30] which gets its intelligence from labeled data. The KNN then tries to classify unlabeled data item based on the category of the majority of most similar training data items known as K. The similarity between two data items in KNN, can be determined with the Euclidean distance of the various respective feature vectors of the data item. Another method which was mostly used is Bayesian Network (BN). BN is a probabilistic classifier algorithm, based on the assumption that, related pair of features used for determining an outcome are independent of each other and equal[30]. There are two commonly used methods of BN for classifying text, thus the multivariant Bernoulli and multinomial models. KNN and BN algorithms were mostly used based on their comparatively higher detection accuracy. For instance, in an experimental assessment of KNN and BNN for security countermeasures of internal threats in healthcare, both KNN and BN had over 90% accuracy. BN performed better (94%) than the KNN (93%). In a related study[39], the KNN method was found to have higher detection rate with high true positive rates and low false positive rate. The major issue with KNN in the context of healthcare staff security generated data is the lack of appropriate labeled data [10, 6, 18]. Within the healthcare setting, emergencies often dictate needs. In such situations, broader accesses for resources are normally allowed, making it challenging for reliable labeled data [18, 10, 6]. Therefore, in adopting KNN for empirical studies, the availability of appropriate labeled data should be considered but, in the absence of labeled data, unsupervised clustering methods such as K means clustering could also be considered [6].

5.5.2 Input data, features, sources, Ground Truth, data format and nature of data

The input data which was mostly used include EHR logs and Network data. A study which was conducted by Yeng et al., for observational measures towards profiling healthcare staffs' security practices, identified various sources including EHR logs, browser history, network logs, and patterns of keystroke dynamics [41]. Most EHR systems uses an emergency access control mechanism, known as "break the glass "or self-authorization" [31]. This enables healthcare staffs, to access patients' medical records during emergency situations without passing through conventional procedures for access authorization. A study into access control methods in Norway [31] revealed that about 50% of 100,000 patients records were accessed by 12,0000 healthcare staffs (representing about 45% of the users) through self-authorization. In such a scenario, EHR remains a vital source for analyzing for deviations of required healthcare security practices. Regarding Ground Truth, it refers to the base-line, often used for training algorithms [34]. The detection efficiency of the algorithms can be negatively impacted if the accuracy of the ground-truth is low. As shown in Table 6, various methods such as similarity measures, observed data and historical methods were used. Similarity measure compares security practices with other healthcare professionals who have similar security practices. Observed measure is a control approach of obtaining the ground truth whereby some users were observed to conduct their security practices under a supervised, required security practices [39]. But the historical data basically relied on past records with a trust that, the data is reliable enough for training set. These methods can be assessed for adoption in related studies. EHR contains most of the features which were identified in this review as shown in Table 5.8. Features such as patients ID, Actions, and User ID are primary features in EHR logs. The actions of the users such as deletion, inserting, updating and various routes such as diagnosis, prescriptions, and drugs dispensing can be tracked in EHR logs [**?**].

5.5.3 Application Scenario and Privacy preserving log analysis

The application of AI methods to analyze big data, generated by healthcare professional security practice, is a reactive approach. With such approaches, the primary aim is to determine deviations or outliers in healthcare security practices and further process these anomalies for possible malicious activities. As most of the algorithms were applied for anomaly detection (60%), such methods can be used to initially detect outliers. Deep leaning methods such as BN can then be used to further analyze the outliers for possible intrusions. This would help in privacy preserving at the same time while saving resources. Privacy preserving in data mining provides method to ef-

ficiently analyze data while shielding the identifications of the data subjects in a way to respect their right to privacy. For instance, limited number of less sensitive features can be used with KNN-based algorithms and if there exist outliers, BN methods can then be applied on only large number of the outliers to further assess these anomalies. In the review, deidentification, tokenization and sensitive data removals were some of the methods adopted to preserve privacy.

5.5.4 Conclusion

Based on the galloping rate of data breaches in healthcare, Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) project was initiated to observe, model and analyze healthcare staffs' security practices. One of the approaches in the project is the adoption of AI methods for modeling and analyzing healthcare staffs' generated security practice data. This systematic review was then conducted to identify, asses and analyze the appropriate AI methods and data sources. Out of about 130 articles which were initially identified in the context of human-generated healthcare data for security measures in healthcare, 15 articles were found to meet this inclusion and exclusion criteria. After the assessment and analysis, various methods such as KNN, Bayesian Network and Decision Trees (C4.5) algorithms were mostly applied on Electronic Health Records (EHR) Logs and Network logs with varying input features of healthcare staffs' security practices.

With these algorithms, security practice of healthcare staffs, can then be studied. Deviations of security practices from required healthcare staffs' security behavior can be examined to define appropriated incentives towards improving conscious care security practice. Analyzing healthcare staff security practice with AI seems to be a new research focus area and this resulted into the inclusion of only 15 articles in this study. Among these included articles, there were no adequate recorded performance scores. As a result, the study could not adequately perform a comparative assessment of the performance of the identified algorithms. Future work would include development of a framework and a practical assessment of the performance of these methods towards implementation in real healthcare staffs' generated logs.

5.6 Bibliography

[1] Network firewalls: Perimeter defense - dummies, 2018. 138

[2] ADEVA, J. J. G., AND ATXA, J. M. P. Intrusion detection in web applications using text mining. *Eng. Appl. Artif. Intell. 20*, 4 (2007), 555–566. 148

[3] AMÁLIO, N., AND SPANOUDAKIS, G. From monitoring templates to security monitoring and threat detection. In *Proceedings of the Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2008, August 25-31, 2008, Cap Esterel, France* (2008), A. Cotton, O. Dini, A. F. Gómez-Skarmeta, M. Ion, M. Popescu, and M. Takesue, Eds., IEEE Computer Society, pp. 185–192. 148

[4] ASFAW, B., BEKELE, D., ESHETE, B., VILLAFIORITA, A., AND WELDEMARIAM, K. Host-based anomaly detection for pervasive medical systems. In *CRiSIS 2010, Proceedings of the Fifth International Conference on Risks and Security of Internet and Systems, Montreal, QC, Canada, October 10-13, 2010* (2010), IEEE Computer Society, pp. 1–8. 147

[5] BODDY, A., HURST, W., MACKAY, M., AND RHALIBI, A. E. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 148

[6] BODDY, A., HURST, W., MACKAY, M., AND RHALIBI, A. E. A hybrid density-based outlier detection model for privacy in electronic patient record system, 2019. 148, 151

[7] BODDY, A. J., HURST, W., MACKAY, M., AND EL RHALIBI, A. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 13, 15, 147, 148, 200, 201, 217, 227, 228

[8] BOSE, B., AVASARALA, B., TIRTHAPURA, S., CHUNG, Y., AND STEINER, D. Detecting insider threats using RADISH: A system for real-time anomaly detection in heterogeneous data streams. *IEEE Systems Journal 11*, 2 (2017), 471–482. 139, 140

[9] CANNOY, S. D., AND SALAM, A. F. A framework for health care information assurance policy and compliance. *Commun. ACM 53*, 3 (2010), 126–131. 138

[10] CHANDRA, S., RAY, S., AND GOSWAMI, R. T. Big data security in healthcare: Survey on frameworks and algorithms, 2017. 141, 151

[11] CHEN, Y., AND MALIN, B. A. Detection of anomalous insiders in collaborative environments via relational analysis of access logs. In *First ACM Conference on Data and Application Security and Privacy, CODASPY 2011, San Antonio, TX, USA, February 21-23, 2011, Proceedings* (2011), R. S. Sandhu and E. Bertino, Eds., ACM, pp. 63–74. 148

[12] CHEN, Y., NYEMBA, S., AND MALIN, B. A. Detecting anomalous insiders in collaborative information systems. *IEEE Trans. Dependable Secur. Comput. 9*, 3 (2012), 332–344. 148

[13] CHEN, Y., NYEMBA, S., ZHANG, W., AND MALIN, B. A. Specializing network analysis to detect anomalous insider actions. *Security Informatics 1*, 1 (2012), 5. 140, 272

[14] CONNOLLY, L. Y., LANG, M., GATHEGI, J., AND TYGAR, D. J. Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security* (2017). 138

[15] COSTANTE, E., FAURI, D., ETALLE, S., DEN HARTOG, J., AND ZANNONE, N. A hybrid framework for data loss prevention and detection. In *2016 IEEE Security and Privacy Workshops, SP Workshops 2016, San Jose, CA, USA, May 22-26, 2016* (2016), IEEE Computer Society, pp. 324–333. 147, 148

[16] E-HELSE, DIREKTORATET FOR. Code of conduct for information security and data protection in the healthcare and care services sector, 2018. 142

[17] GAFNY, M., SHABTAI, A., ROKACH, L., AND ELOVICI, Y. Detecting data misuse by applying context-based data linkage, 2010. 139, 140

[18] GATES, C. S., LI, N., XU, Z., CHARI, S. N., MOLLOY, I., AND PARK, Y. Detecting insider information theft using features from file access logs. In *Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II* (2014), M. Kutylowski and J. Vaidya, Eds., vol. 8713 of *Lecture Notes in Computer Science*, Springer, pp. 383–400. Available from: https://doi.org/10.1007/978-3-319-11212-1_22. 151

[19] GHAFIR, I., HUSÁK, M., AND PRENOSIL, V. A survey on intrusion detection and prevention systems. 140

[20] GHEYAS, I. A., AND ABDALLAH, A. E. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics 1* (2016). 140

[21] GUPTA, S., HANSON, C., GUNTER, C. A., FRANK, M., LIEBOVITZ, D. M., AND MALIN, B. A. Modeling and detecting anomalous topic access. In *2013 IEEE International Conference on Intelligence and Security Informatics, Seattle, WA, USA, June 4-7, 2013* (2013), K. Glass, R. Colbaugh, A. Sanfilippo, A. Kao, M. Gabbay, C. D. Corley, J. Li, L. Khan, A. Wynne, L. Coote, W. Mao, D. Zeng, and A. Yaghoobi, Eds., IEEE, pp. 100–105. 148

[22] HEALTHITSECURITY. Incentivize cybersecurity best practices for data security, 2017. Available from: https://healthitsecurity.com/

news/incentivize-cybersecurity-best-practices-for-data-security. 138

[23] HUMER, C., AND FINKLE, J. Your medical record is worth more to hackers than your credit card, 2014. 138

[24] HUMER, C., AND FINKLE, J. Your medical record is worth more to hackers than your credit card. *Reuters. com US Edition 24* (2014). 138

[25] ISLAM, M., HASAN, M., WANG, X., GERMACK, H., AND NOOR-E-ALAM, M. A systematic review on healthcare analytics: Application and theoretical perspective of data mining. *Healthcare 6* (2018), 54. 140

[26] JIANG, F., JIANG, Y., ZHI, H., DONG, Y., LI, H., MA, S., WANG, Y., DONG, Q., SHEN, H., AND WANG, Y. Artificial intelligence in healthcare: past, present and future. *BMJ* (2017). 141

[27] LI, X., XUE, Y., AND MALIN, B. Detecting anomalous user behaviors in workflow-driven web applications. In *2012 IEEE 31st Symposium on Reliable Distributed Systems* (2012), IEEE, pp. 1–10. 148, 202

[28] PIERROT, D., HARBI, N., AND DARMONT, J. Hybrid intrusion detection in information systems. in 2016 International Conference on Information Science and Security (ICISS), 2016. 148

[29] PREDD, J. B., PFLEEGER, S. L., HUNKER, J., AND BULFORD, C. Insiders behaving badly. *IEEE Secur. Priv. 6*, 4 (2008), 66–70. 138

[30] PRISMA. Prisma, 2018. Available from: http://www.prisma-statement.org/. 142

[31] RØSTAD, L., AND EDSBERG, O. A study of access control requirements for healthcare systems based on audit trails from access logs. In *22nd Annual Computer Security Applications Conference (ACSAC 2006), 11-15 December 2006, Miami Beach, Florida, USA* (2006), IEEE Computer Society, pp. 175–186. 152, 201, 202, 217, 225, 226, 247

[32] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Comput. Secur. 53* (2015), 65–78. 138

[33] SHABAN-NEJAD, A., MICHALOWSKI, M., AND BUCKERIDGE, D. L. Health intelligence: how artificial intelligence transforms population and personalized health. *Nature Medicine 1* (2018). 141

[34] SMYTH, P., FAYYAD, U. M., BURL, M. C., PERONA, P., AND BALDI, P. Inferring ground truth from subjective labelling of venus images. In *Advances in Neural Information Processing Systems 7, [NIPS Conference, Denver, Colorado, USA, 1994]* (1994), G. Tesauro, D. S. Touretzky, and T. K. Leen, Eds., MIT Press, pp. 1085–1092. 152

[35] TCHAKOUCHT, T. A., EZZIYYANI, M., JBILOU, M., AND SALAÜN, M. Behavioral appraoch for intrusion detection. In *12th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2015, Marrakech, Morocco, November 17-20, 2015* (2015), IEEE Computer Society, pp. 1–5. 147, 148

[36] VERISON. Data breaches report. 2019, 2019. Available from: `https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf`. 138

[37] VIHINEN, M., AND SAMARGHITEAN, C. Medical expert systems. *Current Bioinformatics 3*, 1 (2008), 56–65. 141

[38] WAHL, B., COSSY-GANTNER, A., GERMANN, S., AND SCHWALBE, N. R. Artificial intelligence (ai) and global health: how can ai contribute to health in resource-poor settings? *BMJ Global Health 3* (2018), e000798. 141

[39] WALKER-ROBERTS, S., HAMMOUDEH, M., AND DEHGHANTANHA, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access 6* (2018), 25167–25177. 139, 140, 151

[40] WESOLOWSKI, T. E., PORWIK, P., AND DOROZ, R. Electronic health record security based on ensemble classification of keystroke dynamics. *Applied Artificial Intelligence 30*, 6 (2016), 521–540. 148

[41] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[42] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 11, 15, 22, 138, 200, 217, 224, 236, 273, 274, 404, 406, 407, 409, 414, 426, 442, 491, 498

[43] ZHANG, H., MEHROTRA, S., LIEBOVITZ, D. M., GUNTER, C. A., AND MALIN, B. A. Mining deviations from patient care pathways via electronic medical record system audits. *ACM Trans. Management Inf. Syst. 4*, 4 (2013), 17:1–17:20. 138, 148

[44] ZIEMNIAK, T. Use of machine learning classification techniques to detect atypical behavior in medical applications. In *Sixth International Conference on IT Security Incident Management and IT Forensics, IMF 2011, Stuttgart, Germany, May 10-12, 2011* (2011), H. Morgenstern, R. Ehlert, S. Frings, O. Göbel, D. Günther, S. Kiltz, J. Nedon, and D. Schadt, Eds., IEEE Computer Society, pp. 149–162. 148

Chapter 6

Artificial Intelligence–Based Framework for Analyzing Health Care Staff Security Practice: Mapping Review and Simulation Study

Prosper Kandabongee Yeng ; Livinus Obiora Nweke; Bian Yang ; Muhammad Ali Fauzi; Einar Arthur Snekkenes

Abstract

Background:

Blocklisting malicious activities in health care is challenging in relation to access control in health care security practices due to the fear of preventing legitimate access for therapeutic reasons. Inadvertent prevention of legitimate access can contravene the availability trait of the confidentiality, integrity, and availability triad, and may result in worsening health conditions, leading to serious consequences, including deaths. Therefore, health care staff are often provided with a wide range of access such as a "breaking-the-glass" or "self-authorization" mechanism for emergency access. However, this broad access can undermine the confidentiality and integrity of sensitive health care data because breaking-the-glass can lead to vast unauthorized access, which could be problematic when determining illegitimate access in security practices.

Objective: A review was performed to pinpoint appropriate artificial intelligence (AI) methods and data sources that can be used for effective modeling and analysis of health care staff security practices. Based on knowledge obtained from the review, a framework was developed and implemented with simulated data to provide a comprehensive approach toward effective modeling and analyzing security practices of health care staff in real access logs.

Methods: The flow of our approach was a mapping review to provide AI methods, data sources and their attributes, along with other categories as

input for framework development. To assess implementation of the framework, electronic health record (EHR) log data were simulated and analyzed, and the performance of various approaches in the framework was compared.

Results: Among the total 130 articles initially identified, 18 met the inclusion and exclusion criteria. A thorough assessment and analysis of the included articles revealed that K-nearest neighbor, Bayesian network, and decision tree (C4.5) algorithms were predominantly applied to EHR and network logs with varying input features of health care staff security practices. Based on the review results, a framework was developed and implemented with simulated logs. The decision tree obtained the best precision of 0.655, whereas the best recall was achieved by the support vector machine (SVM) algorithm at 0.977. However, the best F1-score was obtained by random forest at 0.775. In brief, three classifiers (random forest, decision tree, and SVM) in the two-class approach achieved the best precision of 0.998.

Conclusions: The security practices of health care staff can be effectively analyzed using a two-class approach to detect malicious and nonmalicious security practices. Based on our comparative study, the algorithms that can effectively be used in related studies include random forest, decision tree, and SVM. Deviations of security practices from required health care staff's security behavior in the big data context can be analyzed with real access logs to define appropriate incentives for improving conscious care security practice.

6.1 Introduction

6.1.1 Background

Unlike other sectors, the health care sector cannot afford to implement stricter control for accessing sensitive health care information for therapeutic purposes. Despite the recognized need to provide tighter security measures in controlling access, there is also the need to strike a balance for allowing legitimate access to health care data for therapeutic reasons [4, 47]. In access control management in health care, access to personal health data and personal data filing systems for therapeutic purposes must be granted following a specific decision based on "the completed or planned implementation of measures for the medical treatment of the patient" [18]. Therefore, access must only be granted to those with official needs[18, 60]. While providing restrictions against unauthorized access, there are some provisions for following the availability trait of the confidentiality, integrity, and availability (CIA) triad during emergency situations. These include the provision for self-authorization. Self-authorization, or "break-the-glass," is a "technical measure which has been established for health personnel to be able to gain

access to personal health data and personal data as and when necessary" [4]. However, access through self-authorization must be verified for abuse, and clear misuse must be followed up as a data breach [18, 41].

The challenge remains in detecting misuse over a broad range of access [4, 47]. A broad range of access via self-authorization results in tones of variant data known as "big data" [6], making it complex to manually determine legitimate access. However, in light of the recent increase in data breaches within health care, it has become necessary to adopt state-of-the-art methods to determine anomalous access. In the Healthcare Security Practice Analysis, Modeling, and Incentivization (HSPAMI) project [65], data-driven and artificial intelligence (AI) approaches were identified and adopted to aid in modeling and analyzing health care staff's security practices in their access control logs [65]. AI is based on algorithms in computer science that can be used for analyzing complex data to draw meaningful patterns and relationships toward decision making [25]. The aim of this study was to understand anomaly practices in health care in the context of big data and AI, and to determine the security practice challenges often faced by health care workers while performing their duties. The results will provide knowledge to serve as a guide for finding better approaches to security practice in health care. However, there are different types of data sources and AI methods that can be used in this approach [65]. We therefore adopted a review methodology to first detail various types of dimensions, including the data sources and AI methods, which can be adopted in related studies.

According to Verizon, the health care sector globally experienced approximately 503 data breaches in 2018, which resulted in the compromise of up to 15 million records [60, 40]. This figure was triple the number of data breaches recorded in 2017. In addition, the number of records compromised within the health care sector in 2019 far exceeded that recorded in 2018 [40]. Unfortunately, more than half of these data breaches were perpetuated by insiders [40]. The report opined that approximately 83% of the adversaries were motivated by financial gains, 3% were due to convenience, 3% were due to grudges, and 2% were a result of industrial espionage. The current situation implies that the number of data breaches within the health care sector has surpassed that of the financial sector and almost equals those of other public sectors.

This situation has raised concerns among relevant stakeholders, and many are wondering the reasons behind the spike in the number of data breaches within the health care sector. Some of these reasons can be easily deduced because health care data have economic value and as such represent a possible target for malicious actors [52, 26]. Moreover, health care data have scientific and societal value that makes them very attractive for cyber criminals. In fact, Garrity et al [20] indicated that patient medical records are sold for approximately US $1000 on the dark web. Another reason for data

breaches within health care is the lack of health care personnel. The few health care personnel are more interested in their core health care duties and have little time to handle health care information security issues. This situation provides cyber criminals with the opportunity to exploit health care systems.

Although there have been improvements in technical measures, such as firewalls, intrusion detection and prevention systems, antivirus software, and security governance configurations, the development of a "human firewall" has not been considered [11, 48]. The "human firewall" refers to the information security conscious care behavior of insiders [58]. However, this concept has not received equal attention as devoted to technical measures, and thus cyber criminals seek to exploit it for easy access [64]. Health care insiders have access privileges that enable them to provide therapeutic care to patients; however, through errors or deliberate actions, they can compromise the CIA of health care data. It is also possible for an attacker to masquerade as an insider to compromise health care data through social engineering and other methods [46, 44].

Access control mechanisms within the health care sector are usually designed with a degree of flexibility to facilitate efficient patient management [37]. Even though such design considerations are vital and can meet the availability attribute of the CIA, they make health care systems vulnerable. This is because flexibility can be abused by insiders [38]. In addition, an attacker who could obtain an insider's access privilege can exploit this flexibility to have broader access. A successful data breach could have many consequences such as denial of timely medical services, corrosion of trust between the patient and health care providers, breaches to an individual's privacy [35], and huge fines to health care providers by national and international regulatory bodies. The general objective of this study was to determine an effective way of modeling and analyzing health care logs. A review was first performed to retrieve appropriate data sources and their features in addition to identifying the AI methods that can best be used to determine irregularities in security practices among health care workers.

6.1.2 Prior Studies

The security practices of health care staff include how health care professionals respond to security controls and measures for achieving the CIA goals of health care organizations [47, 60, 41]. Health care professionals are required to conduct their work activities in a security-conscious manner to maintain the CIA of the health care environment [11]. For instance, borrowing access credentials could jeopardize the purpose of access control for authorized users and legitimate access. Additionally, the inability to understand social engineering scammers' behavior can lead to health care data breaches [65].

Various approaches can be adopted to observe, model, and analyze health care professionals' security practices. A perception and sociocultural context can be adopted by analyzing the security perception, and social, cultural, and sociodemographic characteristics of health care staff in the context of their required security practices[65, 66]. In addition, an attack-defense simulation can be used to measure how health care staff understand social engineering–related tricks. Furthermore, a data-driven approach with AI methods could be adopted to understand the security behavior of each health care professional in the context of big data, since AI is most appropriate for analyzing complex data sets with high volume, variety, velocity, and veracity [25]. The findings can then help decision makers to introduce appropriate incentive methods and solve issues that hinder sound information security practice toward enhancing conscious care behavior.

Advances in computational and data science, along with engineering innovations in medical devices, have prompted the need for the application of AI in the health care sector [66, 49, 68, 34]. This has the potential to improve health care delivery and revolutionize the health care industry. AI can be referred to as the use of complex algorithms and software to imitate human cognitive functions [68, 34, 30]. AI involves the application of computer algorithms in the process of extracting meaning from complicated data and making intelligent decisions without direct human input [68, 34]. AI is increasingly impacting every aspect of our lives, and the health care sector is no exception. In recent years, the health care sector experienced massive AI deployments in the bid to improve overall health care delivery. We here rely on the classification of the application of AI in health care described by Wahl et al [55] to briefly discuss the deployment of AI in health care.

According to Wahl et al [55], the deployment of AI in the health care sector has been classified to include expert systems, machine learning, natural language processing, automated planning and scheduling, and image and signal processing [55]. Expert systems are AI programs that have been trained with real cases to execute complicated tasks [54]. Machine learning employs algorithms to identify patterns in data and learn from them, and its applications can be grouped into three categories: supervised learning, unsupervised learning, and reinforcement learning[34, 55]. Natural language processing facilitates the use of AI to determine the meaning of a text by using algorithms to identify keywords and phrases in natural language. Automated planning and scheduling is an emerging field in the use of AI in health care that is concerned with the organization and prioritization of the necessary activities to obtain the desired aim [55]. Image and signal processing involves the use of AI to train information extracted from a physical occurrence (images and signals) [55].

The common characteristic of all these applications is the utilization of massive data that are being generated in the health care sector to make bet-

ter informed decisions. For instance, the collection of data generated by health care staff has been used for disease surveillance, decision support systems, detecting fraud, and enhancing privacy and security [12]. In fact, the code of conduct for the Norwegian health care sector requires the appropriate storage and protection of access logs of health care information systems for security reasons [11]. Health care staff's access to the network or electronic health records (EHR) leaves traces of their activities, which can be logged and reconstructed to form their unique profiles [11, 60]. Therefore, appropriate AI methods can be used to mine such logs to determine the unique security practices of health care staff. Such findings can support management in adapting suitable incentivization methods toward improving security-conscious care behavior in health care. Therefore, the aim of this study was to explore the appropriate AI methods and data sources that can be used to observe, model, and analyze the security practices of health care staff.

HSPAMI is an ongoing research project with one aspect involving the modeling and analysis of data with AI methods to determine the security practices of health care staff toward improving their security-conscious care behavior. In analyzing health care–related data, there is a need to consider details of the methods and data sources in view of the unique and critical nature of the sector. In a related study, Walker-Roberts et al [56] performed a systematic review of "the availability and efficacy of countermeasures to internal threats in health care critical infrastructure." Among various teams, few machine learning methods were identified to be used for intrusion detection and prevention. The methods that were identified are Petri net, fuzzy logic, k-nearest neighbor (KNN), decision tree (RADISH system) [56, 10, 19], and inductive machine learning methods [56, 10, 15]. In a similar way, Islam et al [28] performed a systematic review on data mining for health care analytics. Categories such as health care subareas; data mining techniques; and the types of analytics, data, and data sources were considered in the study. Most of the data analysis was focused on clinical and administrative decision-making. The data sources were mostly human-generated from EHRs. Gheyas et al [23] also explored related methods in their systematic review and meta-analysis [23].

Even though the studies of Walker-Roberts et al [56] and Islam et al [28] were in the health care context, details of the algorithms and data sources were not considered. For instance, the features of the data sources and algorithm performance methods were not deeply assessed in their studies. Additionally, these studies were general and not specific to health care [23, 32], and therefore the unique challenges within the health care environment were not considered. To this end, this study explored AI methods and data sources in health care that can be efficiently used for modeling and analyzing health care professionals' behavior. The terms "health care pro-

fessionals" and "health care staff" are used interchangeably in this paper, which include, but are not limited to, nurses, physicians, laboratory staff, and pharmacies who access patient records for therapeutic reasons.

6.1.3 Scope, Problem Specification, and Contribution

Following the recent increase in data breaches in health care, our research group is working on the HSPAMI project, which was initiated to measure the information security practice level of health care staff [65, 66]. The results will help provide better approaches for incorporating conscious care behavior among health care staff. The HSPAMI project has already identified various approaches to include psychosociocultural context attack and defense simulations in a social engineering context along with data-driven AI approaches [65].

The main goal is to demonstrate how health care security practices can be analyzed to determine anomalous and malicious activities in the context of data-driven and AI approaches. Therefore, the specific objectives of this study were to identify, assess, and analyze the state-of-the-art data-driven attributes and AI methods along with their design strategies and challenges. A framework for analyzing health care security practice in the context of data-driven and AI methods was also developed and evaluated. The broad goal was to enable analysis of real logs of health care professionals' security practices in the context of big data and human-generated data logs. Therefore, the psychosociocultural context and attack-defense simulations are beyond the scope of this paper.

Some details of data sources and AI methods that can be used in this study were not provided in previous related work [56, 10, 19, 15, 28], which raised several questions for our research: Among the various data sources that are generated by health care staff, which is the most appropriate to be used in analyzing the security practice? Which AI methods have been pinpointed to be suitable for use in modeling and analyzing health care security practice? What evaluation techniques are most appropriate in this context, and how were these methods adjusted to curtail biases amid various access points, such as self-authorization during emergency care scenarios and the busy schedules of health care staff? To answer these questions, we first performed a mapping review [63] toward identifying, modeling, and analyzing health care staff–generated access logs and AI methods to enhance security practice. This work represents an extended version of our previous work, with the additions being a design and framework evaluation.

6.2 Methods

6.2.1 Literature Review

Various types of systematic studies exist [33, 9, 31, 42], including a systematic mapping study, scoping review, and systematic literature review. Systematic mapping studies review topics with a broader scope by categorizing the identified research articles into specific areas of interest. Systematic mapping studies have general research questions with the objective to determine research trends or the state-of-the-art studies. By contrast, the objective of a systematic literature review is to accumulate data and therefore has a more specific research focus. To this end, a systematic mapping study was adopted in this work[33, 9]. Based on the results, we developed a framework that was evaluated with simulated log data.

Although we did not restrict the article search to a specific time frame, we performed the literature search between June 2019 and December 2019 with the Google Scholar, Science Direct, Elsevier, IEEE Explore, ACM Digital, Scopus, Web of Science, and PubMed databases. Different keywords were used, including "healthcare," "staff," "employee," "information security," "behavior," "practice," "threat," "anomaly detection," "intrusion detection," "artificial intelligence," and "machine learning." To ensure a high-quality searching approach, the keywords were combined using the Boolean functions "AND," "OR," and "NOT." For instance, the following search string was generated in PubMed:

((Intrusion[All Fields] AND Detection[All Fields]) OR (Anomaly[All Fields] AND Detection[All Fields])) AND ("health"[MeSH Terms] OR "health"[All Fields]) AND (("artificial intelligence"[MeSH Terms] OR ("artificial"[All Fields] AND "intelligence"[All Fields]) OR "artificial intelligence"[All Fields]) OR ("machine learning"[MeSH Terms] OR ("machine"[All Fields] AND "learning"[All Fields]) OR "machine learning"[All Fields])) AND ("information"[All Fields] AND Security[All Fields]) AND (("behavior"[All Fields] OR "behavior"[MeSH Terms] OR "behavior"[All Fields]) OR "practice"[All Fields]).

Peer-reviewed articles were considered. The inclusion and exclusion criteria were developed based on the objective of the study and through rigorous discussions among the authors.

Basic selection was performed by initially skimming through the titles, abstracts, and keywords to retrieve records that were in line with the inclusion and exclusion criteria. Duplicates were filtered out, and articles that seemed relevant, based on the inclusion and exclusion criteria, were fully read and evaluated. Each of the authors independently read and assessed all of the selected articles and judged either to be included or excluded. Using the inclusion and exclusion criteria as a guideline, discrepancies were discussed and resolved among the authors. Other appropriate articles were also retrieved using the reference list of accepted literature. Figure 12.1

shows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) [45] flowchart of article screening and selection.

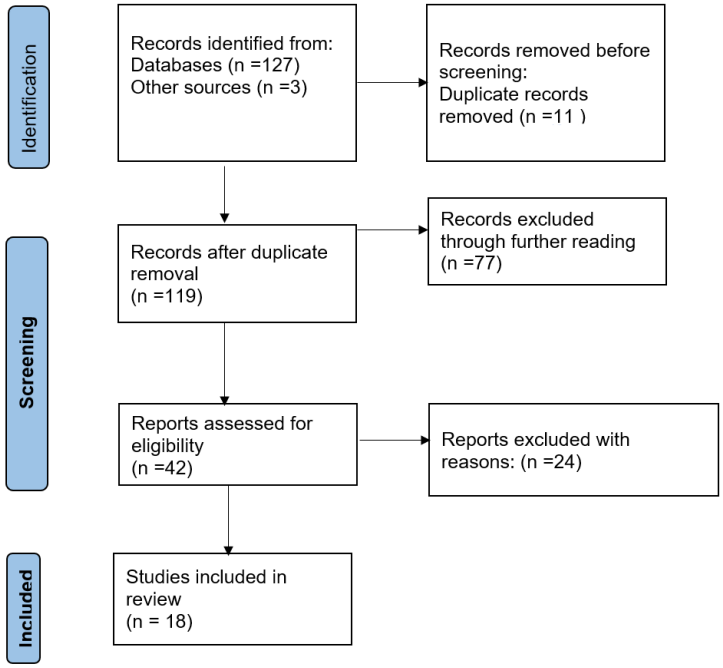


Figure 6.1: Flowchart of the systematic review process.

6.2.2 Inclusion and Exclusion Criteria

For an article to be included in the review, it had to be related to anomaly detection or intrusion detection in health care using AI methods with health care professional–generated access log data or patterns. Any other article outside the above scope (such as articles related to medical cyber-physical devices, body area networks, and similar), along with articles published in languages other than English, were excluded.

6.2.3 Data Collection and Categorization

The data collection and categorization methods were developed based on the study objective, and thorough literature reviews and discussions among the authors. The categories were defined exclusively to assess, analyze, and evaluate the study objectives, which are summarized in Table 12.1.

Table 6.1: Data categories and their exclusive definitions

Category	Definition	Examples
Type of AIa method	Explicit machine learning methods	Support vector machine, Bayesian network
Type of input	Features used by the algorithm	Access location, time, failed login attempts
Input sources	Type of access log data used in the study	Browser history, network logs, host-based activity logs, EHR logs
Data format, type, size, and data source	File formats	XML, comma separated value (CSV)
Input preprocessing	Defines how the data were preprocessed and how missing and corrupted input data were handled	Structured vs unstructured
Security failures	Context in which the algorithm was implemented	Intrusion or anomaly detection
Ground truth	Type of training set used in training the model	Login and logout time, average number of patient records accessed
Privacy approach	Defines the privacy method used to safeguard the privacy rights of individuals who contributed to the data source	Message Digest 5 (MD5), Secure Hash Algorithm (SHA)-3
Performance metrics or evaluation criteria	Measures used to assess the accuracy of the study	Specificity, sensitivity, receiver operating characteristic curve
Nature of data sources	Specifies whether the data used were synthetic or real data	Real data, simulated data

6.2.4 Literature Evaluation and Analysis

The selected articles were assessed, analyzed, and evaluated based on the categories defined in Table 12.1 The analysis was performed on each of the categories (eg, type of AI method, type of input, input source, preprocessing, learning techniques, performance methods) to evaluate the state-of-the-art approaches. Percentages of the attributes of the categories were calculated based on the total number of counts (n) of each type of attribute. Some studies used multiple categories; therefore, the number of counts of these categories exceeded the total number of articles of these systems presented in the study.

6.3 Results

6.3.1 Review Findings

6.3.1.1 Articles Retrieved

After searching the various online databases, a total of 130 records were initially identified following the guidelines of the inclusion and exclusion criteria in the reading of titles, abstracts, and keywords. A further assessment of these articles through skimming of the objective, method, and conclusion sections led to an exclusion of 77 articles that did not meet the defined inclusion criteria. After removing duplicates, 42 articles were fully read and judged. After full-text reading, a total of 18 articles were included in the study and analysis (Figure 12.1).

6.3.1.2 Algorithms

The main findings of the reviewed articles and their related categorizations such as algorithms, features, and data sources are shown in Figure 12.2. The algorithms, features, data sources, and application domains were the most frequent categorizations in the review; the study column presents the sources of each of these categories.

The algorithms that were most commonly used for analyzing security practice in the review are shown in Table 12.2. The KNN method was the most frequently used, followed by the Bayesian network and C4.5 decision tree.

6.3.1.3 Features

Table 12.3 shows the unique features identified in the review and their respective counts and proportions. The features that were the most frequently used included user ID, date and time attribute, patient ID, and device identification.

Table 6.2: . Algorithms and their respective proportions among the articles included in the review (N=30)

Algorithm	**Studies, n (%)**	**References**
K-nearest neighbor	5 (17)	[8, 1, 24, 14, 13]
Bayesian network	4 (13)	[8, 1, 3, 57]
Decision tree (C4.5)	3 (10)	[68, 57, 43]
Random forest	2 (7)	[57, 43]
J48	2 (7)	[68, 57]
Support vector machine	1 (3)	[57, 39]
Spectral projection model	1 (3)	[13]
Principal component analysis	1 (3)	[13]
K-means	1 (3)	[52]
Ensemble averaging and a human-in-the-loop model	1 (3)	[7]
Partitioning around Medoids with k estimation (PAMK)	1 (3)	[43]
Distance-based model	1 (3)	[36]
White-box anomaly detection system	1 (3)	[16]
C5.0	1 (3)	[50]
Hidden Markov model	1 (3)	[36]
Graph-based	1 (3)	[67]
Logistic regression	1 (3)	[39]
Linear regression	1 (3)	[39]
Fuzzy cognitive maps	1 (3)	[50]

Table 6.3: . Features used in the reviewed articles (N=65)

Feature	Count, n (%)
User identification	13 (20.0)
Patient identification	11 (16.9)
Device identification	9 (13.8)
Access control	5 (7.7)
Date and time	11 (16.69)
Location	4 (6.2)
Service/route	5 (7.7)
Actions (delete, update, insert, copy, view)	3 (4.6)
Roles	3 (4.6)
Reasons	1 (1.5)

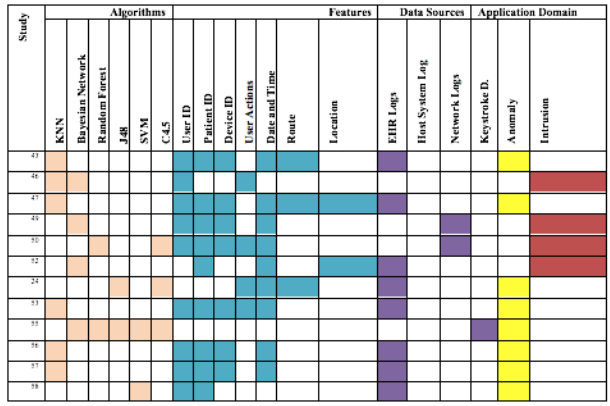


Figure 6.2: Algorithms, features, related data sources, and application domain. KNN: k-nearest neighbor; SVM: support vector machine; EHR: electronic health record.

Table 6.4: Performance methods used in the reviewed studies (N=25).

Performance methods	**Studies, n (%)**
Receiver operating characteristic (ROC) curve	5 (20)
Area under ROC curve	3 (12)
Recall (sensitivity)	5 (20)
Precision	4 (16)
Accuracy	2 (8)
True negative rate (specificity)	3 (12)
F-score	2 (8)
Root mean square error	1 (4)

6.3.1.4 Data Sources

The majority of the data sources were EHR logs (11/18, 61%), followed by host-based logs (2/18, 11%), network logs (4/18, 22%), and keystroke activities (1/18, 5%).

6.3.1.5 Performance Methods

Table 12.4 shows the various types of performance methods that were identified with their respective counts and proportions; recall and receiver operating characteristic curve were the most common metrics applied, whereas F-score and root mean square error were the least commonly applied.

6.3.1.6 Security Failures

The studies in the review were mostly applied for anomaly detection (12/18, 67%) and malicious intrusion detection (6/18, 33%).

6.3.1.7 File Format

Among the 4 articles that reported the file format, 2 (50%) used comma separated values [8, 53] and the other 2 (50%) used the SQL file format [16, 5].

6.3.1.8 Ground Truth

Eight of the 18 articles included in the review reported the ground truth, which was established with similarity measures (3/8, 38%), observed practices (3/8, 38%), and historical data of staff practices (2/8, 25%).

6.3.1.9 Privacy-Preserving Data Mining Approach

Privacy-preserving methods adopted in the included studies were tokenization [8] , deidentification [24], and removal of medical information [68].

6.3.1.10 Nature of Data Source

The majority of studies (15/18, 83%) used real data for analysis, with the remaining (3/18, 17%) using synthetic data.

6.3.2 Framework for Analyzing Health Care Staff Security Practices

Based on the review, a conceptual framework was depicted on how data-driven and AI methods should be adopted to analyze logs of EHRs in security practice (see Figure 12.3). Our review indicated that a security practice analysis typically reveals the anomaly or malicious intrusion pattern of health care staff. Our model therefore has various dimensions such as data sources, preprocessing, feature extraction, the application of AI methods, and possible classes, as shown in Figure 12.3.

The data sources include the network, EHR, or workstation logs. These logs are generated based on health care staff activities in accessing resources such as patients, printers, medical devices, and physical security systems. The logs go through the preprocessing phase [34], such as cleaning and feature selection. The essential features are then selected with appropriate methods, including filter methods, wrapper methods, or the combined filter and wrapper approach. Having obtained the appropriate features, a machine learning method can then be created, trained, and used to detect

patterns of unusual security practices. The various classes that can be deduced in this framework include normal, abnormal, significantly nonmalicious anomaly, and malicious classes. The normal class includes features that follow the flow of each established access process without access aberration. The malicious class consists of features that violate established access flow and may also include excess access, which exceeds the usual trend of users. An example includes a doctor who accesses patient records more than the average daily access, and when the access was not for therapeutic measures. The anomaly nonmalicious class includes accesses that violate the established access flow or that exceed the average daily access of the health care staff; however, in this case, the accesses were for therapeutic purposes. From the framework, three access detection methods were identified for comparison.

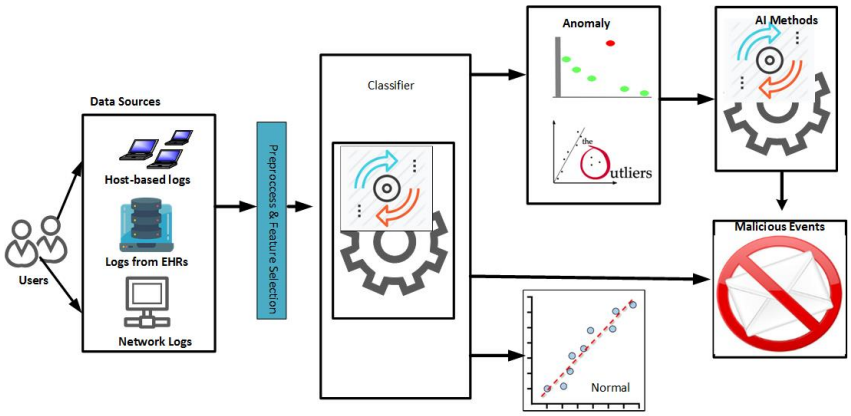


Figure 6.3: Conceptual framework for analyzing the security practices of health care staff. AI: artificial intelligence; EHR: electronic health record

6.3.3 Comparative Analysis of the Framework

The following three access detection methods were compared: (1) two-stage classification, (2) three-class classification, and (3) two-class classification. In the two-stage classification approach, the log data are classified as normal and anomaly. The data determined in the anomaly class from the first stage are further classified into two classes: malicious and nonmalicious (Figure 12.4). In the three-class approach, the log data are classified into normal, nonmalicious anomaly, and malicious, as shown in Figure 12.5. In the two-class approach, the normal and nonmalicious anomaly data are considered as a single "nonmalicious" category. The log data are then classified into nonmalicious and malicious classes, as shown in Figure 12.6.

These three approaches were then compared with nine machine learning methods: multinomial naive Bayes (NB), Bernoulli NB, Gaussian NB, KNN, neural network (NN), logistic regression (LR), random forest (RF), decision tree (DT), and support vector machine (SVM).

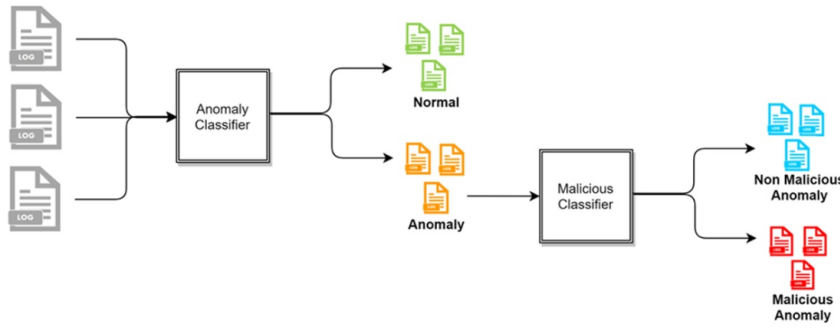


Figure 6.4: Flowchart of two-stage detection.

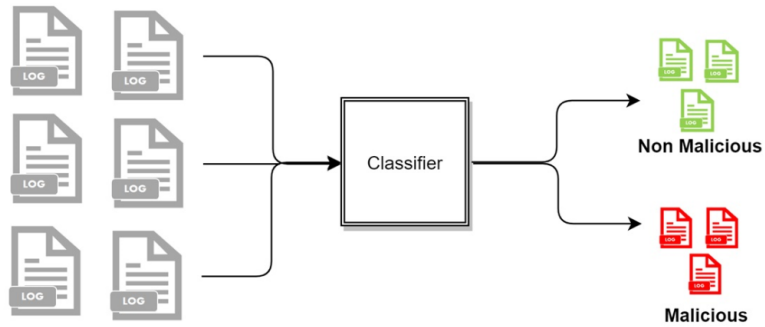


Figure 6.5: Two-class classification.

6.3.4 Simulation of EHR Logs of Health Care Staff Security Practice

The conceptual framework (Figure 12.3) provided direction and guidelines for effective modeling and analysis of health care staff security practices. We hence simulated 1-year access log data of a typical hospital information system from January 1, 2019, to December 31, 2019. Inpatient workflow, outpatient workflow, and emergency care patient workflow were modeled and used in the simulation of the logs as shown in Figure 6.7, Figure 6.8, and

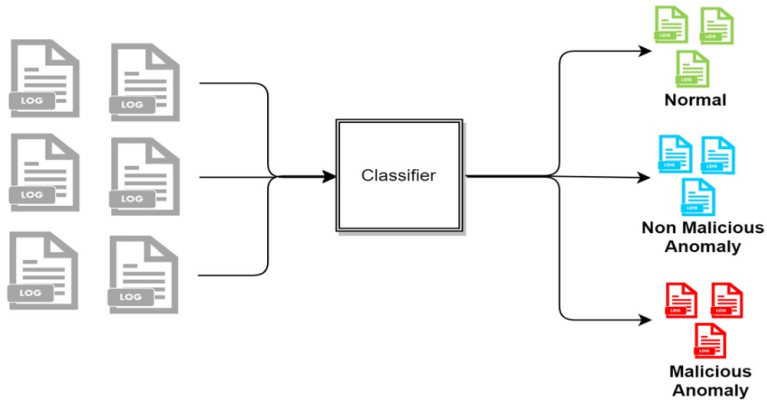


Figure 6.6: Three-class classification.

Figure 6.9, respectively. Five main modules were included in the simulation of the hospital information system: Report, Finance, Patient Management, Laboratory Management, and Pharmacy Management. In the data simulation setting, we used 19 departments and 12 roles with a total of 53 employees. The departments were information technology (3 roles), finance (1 finance officer, 3 finance support staff), administration (1 head of administration, 2 support staff), pharmacy (3 roles), and medical laboratory (5 roles). Outpatient departments included ear-nose-throat (1 doctor, 2 nurses), dentistry (1 dentist, 2 nurses), pediatric unit (1 doctor), orthopedics (1 doctor, 2 nurses), neurology (1 doctor, 2 nurses), gynecology (1 doctor, 2 nurses), endocrinology (1 doctor, 2 nurses), rheumatology (1 doctor, 2 nurses), and cancer (1 doctor, 2 nurses). The inpatient departments included patient wards and the emergency department (2 doctors, 7 nurses).

Two types of shifts were used: a regular shift and three 8-hour shifts. The regular shift is Monday to Friday from 8 AM to 4 PM, whereas the three 8-hour shifts included the following three shifts every day of the week: (1) shift 1, 6 AM to 2 PM; (2) shift 2, 2 PM to 10 PM; and (3) shift 3, 10 PM to 6 AM (next day). The numbers of roles and employees in a regular shift and in the three 8-hour shifts are shown in Table 12.5.

Based on the flows (see Figure 12.6 for an example), we simulated the data and recorded the logs. The logs are considered to be normal data (nonanomaly). We also simulated some abnormal data. The abnormal data were divided into two categories: nonmalicious and malicious. Nonmalicious abnormal data were generated by simulating the "break-the-glass" scenario (eg, access by a doctor from another department due to an emergency) [47], whereas malicious abnormal data were generated by simulating attackers that are assumed to have compromised some users' credentials

Table 6.5: Simulated departments, roles, and staff in a typical hospital.

Department	Roles (number of employees)
Information technology	Head (1), technical support (2)
Finance	Head (1), finance officer (4)
Administration	Head (1), administrative assistants (2)
Laboratory	Head (1), laboratory assistants (5)
Pharmacy	Head (1), pharmacy assistant (2)
Outpatient	
Ear-nose-throat	Doctor (1), nurse (2)
Optometry	Doctor (1), nurse (2)
Dentistry	Doctor (1), nurse (2)
Pediatrics	Doctor (1), nurse (2)
Orthopedics	Doctor (1), nurse (2)
Neurology	Doctor (1), nurse (2)
Gynecology	Doctor (1), nurse (2)
Endocrinology	Doctor (1), nurse (2)
Rheumatology	Doctor (1), nurse (2)
Cancer	Doctor (1), nurse (2)
Inpatient	
Ward 1	Doctor (1), nurse (2)
Ward 2	Doctor (1), nurse (2)
Ward 3	Doctor (1), nurse (2)
Three 8-hour shift	
Emergency	Doctor (2), nurse (2)
Ward 1	Nurse (2)
Ward 2	Nurse (2)
Ward 3	Nurse (2)

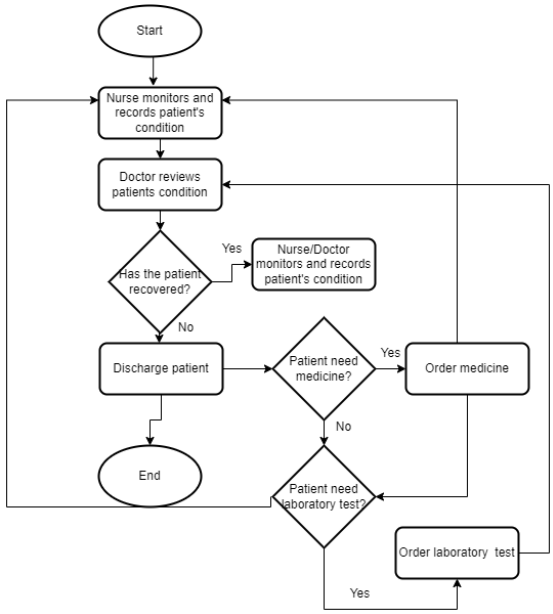


Figure 6.7: Inpatient workflow.

and used them to access patient records (eg, identity theft). In the latter category, the attacker will access more data than legitimate users and often not follow the flows. From this data simulation, 281,886 logs were created with 273,094 normal access, 7647 nonmalicious abnormal access, and 1145 malicious access scenarios. There are 21 fields recorded in this data simulation, as displayed in Table 12.6.

6.3.5 Feature Extraction

To develop the anomaly detection model, including the role classification model, some features were extracted. Each log entry represents a single transaction for a user. To analyze the user activity, the logs from each user were consolidated into a particular period. Every single activity of Doctor A would represent meaningless data points that would be difficult to analyze separately. However, by observing several activities of Doctor A for a particular period, it is easier to perform the anomaly detection task. We processed the log data into 24-hour blocks so that an instance represents the cumulative activity of a user in a single day. As a result, 25,151 instances were extracted from the raw logs, with 24,223 of them being considered normal, 585 considered nonmalicious anomaly, and 343 labeled malicious. Any access

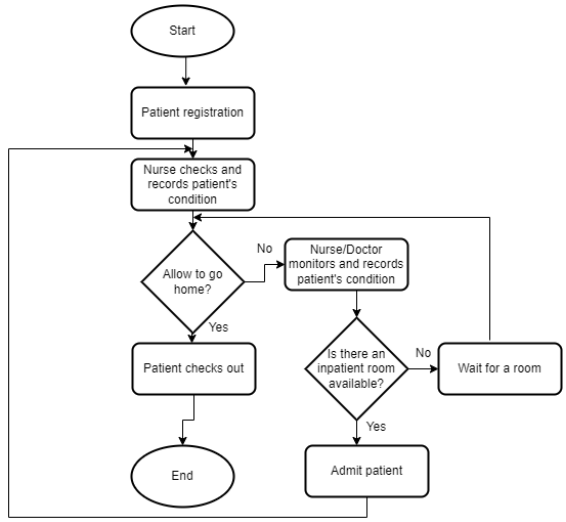


Figure 6.8: Emergency workflow.

that was not for the intention of providing therapeutic functions constitutes malicious access [22]. Therefore, in the logs, malicious data represent all instances that had at least one malicious log access in a single day. The normal data represent all instances in which all of the accesses to the logs are legitimate, and the nonmalicious anomaly data represent the instances that had at least one abnormal log access, but none of them was malicious. These instances were then transformed into features for malicious access detection. Table 12.7shows the features extracted from the data set.

6.3.6 Performance Evaluation for Malicious Detection

For malicious access detection, several measurements, including precision, recall, and F-measures, were identified and used to evaluate the performance. All measurements were calculated based on the confusion matrix displayed in Table 12.8.

True positive (TP) and true negative (TN) are the respective number of features that were correctly predicted. TP represents the malicious data that were correctly predicted as malicious, whereas TN represents the nonmalicious data that were correctly predicted as nonmalicious. False positive (FP), also often called the type I error, is the number of nonmalicious data incorrectly predicted as malicious, and false negative (FN), or the type II error, represents the malicious data incorrectly predicted as nonmalicious. The following are the formulas for each measurement:

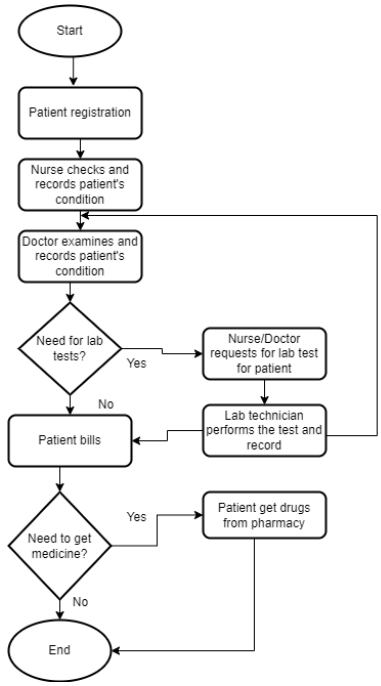


Figure 6.9: Outpatient care workflow.

$$Precision = \frac{TP}{TP + FP} \tag{6.1}$$

$$Recall = \frac{TP}{TP + FN} \tag{6.2}$$

$$F1 = \frac{2 * ([precisionrecall])}{[precision + recall]} \tag{6.3}$$

$$FB = \frac{(1 + \beta 2)(precisionrecall)}{(\beta 2 * precision] + recall)} \tag{6.4}$$

Equation 6.3 is the standard F-score formula where precision and recall have the same weight. If we want to give heavier weight to either precision or recall, we can use equation 6.4. For any positive real number beta (B), equation 6.4 is the general F-measure formula where recall is considered to be more important than precision by a weight of beta (B) [17]. In this work, we also used the F0.5-score and F2-score. F0.5-score means that precision

Table 6.6: Field attributes of simulated access logs of electronic health records.

Attribute	Description
startAccessTime	The time the employee starts to access the patient record: format=day/month/year, hours:minutes:seconds
endAccessTime	The time the employee ends the patient record access: format=day/month/year, hours:minutes:seconds
employeeID	The identification number of the employee who accesses the patient record (eg, record4roleID)
roleID	The role of the employee who accesses the patient record
patientID	The identification number of the patient whose record is being accessed by the employee
activityID	The identification number of the activity (1: Create, 2: Read, 3: Update, 4: Delete)
employeeDepartmentID	The department of the employee who accesses the patient record
employeeorganizationID	The organization of the employee who accesses the patient record
osID	The operating system of the computer used by the employee to access the patient record
deviceID	The identification number of the computer used by the employee to access the patient record
browserID	The browser used by the employee to access the patient record
ipAddress	The IP address of the computer used by the employee to access the patient record
ReasonID	The reason for the employee accessing the patient record (optional)
shiftID	The identification of the shift the employee belongs to on the day of accessing the patient record
shiftStartDate	The start time of the shift the employee belongs to on the day of accessing the patient record
shiftEndDateTime	The end time of the shift the employee belongs to on the day of accessing the patient record
CRUD	The identification code of the activity (C: Create, R: Read, U: Update, D: Delete)
Access Control Status	Access control status
SessionID	The identification of the session access
AccessPatient_Warnings	Warning for unusual access
Module Used	The module accessed by the employee

is considered to be two times more important than recall. In contrast, F2-score means that recall is considered to be two times more important than precision. To compute the F0.5-score, the beta (B) value was substituted with 0.5, whereas the F2-score was calculated by replacing the beta (B) value with 2.

Usually, automatic malicious behavior detection is used as a filter to narrow down the data for further manual investigation. In this case, high recall

Table 6.7: Features and their related descriptions.

Name of feature	**Description**
Number of create	Number of created transactions in a single day
Number of reads	Number of read transactions in a single day
Number of updates	Number of updated transactions in a single day
Number of deletes	Number of deleted transactions in a single day
Number of patient records	Number of accesses to patient records in a single day
Number of unique patients	Number of unique patients' records accessed in a single day
Number of modules	Number of the types of modules in the information system accessed in a single day
Number of report modules	Number of transactions in the report modules in a single day
Number of finance modules	Number of finance modules accessed in a single day
Number of patient modules	Number of transactions in the patient module in a single day
Number of lab modules	Number of transactions in the laboratory module in a single day
Number of pharmacy modules	Number of transactions in the pharmacy module in a single day
Number of outside access	Number of transactions from outside the hospital network in a single day
Number of other browsers	Number of browser types used in a single day
Number of Chrome	Number of Chrome uses in a single day
Number of Internet Explorer	Number of Internet Explorer uses in a single day
Number of Safari	Number of Safari uses in a single day
Number of Firefox	Number of Firefox uses in a single day
Number of browsers	Number of other browsers used in a single day

Table 6.8: Confusion matrix.

Actual	Predicted	
	Malicious	Nonmalicious
Malicious	True positive	False negative
Nonmalicious	False positive	True negative

is preferred so that most of the actual malicious access will not be missed. Therefore, F2 is the better measure for this case. However, if we want to use

the result from automatic malicious behavior detection as the final decision without further manual investigation, high precision is preferred over high recall. By using a high-precision method, almost all of the banned accesses are actually malicious. In contrast, if we use an algorithm that prefers high recall as the final decision-maker, we may ban some legitimate accesses that are mistakenly considered fraudulent. In this case, F1 is the better measure. However, the latter case is rarely applied in the real world since malicious behavior detection is mainly used for a decision support system before further manual investigation.

In this study, we used the logs from January to July as training data, whereas data from August to December were used for testing. The training data were used to train the role classification model, and then this model was used to detect anomalies based on the two proposed approaches. The training data contained a total of 14,558 instances with 13,977 normal instances, 339 nonmalicious anomaly instances, and 242 malicious instances. The testing data consisted of a total of 10,593 instances, with 10,246 normal instances, 246 nonmalicious anomaly instances, and 101 malicious instances.

6.3.7 Experimental Results

The simulation results are summarized in Table 12.9 and Table 6.10. Table 12.9 shows the anomaly detection results from the first stage of two-stage malicious detection. Based on the result, the DT algorithm obtained the best precision (0.655), while the best recall was achieved by SVM (0.977). However, the best F1-score was obtained by RF (0.775). Therefore, the result that was used in the second stage was that obtained from the RF method.

Table 6.9: Anomaly detection results from the first step of two-stage malicious detection

Classifier	**Precision**	**Recall**	**F1**
Multinomial naive Bayesa	0.256	0.107	0.151
Bernouilli naive Bayes	0.256	0.824	0.391
Gaussian naive Bayes	0.256	0.618	0.362
k-nearest neighbor	0.634	0.89	0.74
Neural network.	0.651	0.941	0.77
logistic regression	0.242	0.976	0.387
Random forest.	0.662	0.934	0.775
Decision tree.	0.665	0.924	0.773
Support vector machine.	0.25	0.977	0.399

Table 6.10shows the malicious detection results using three approaches. The two-class approach tended to have better performance than the other

two approaches. The best precision in the two-stage approach was obtained by LR with a perfect value (1.00), and KNN also had perfect precision in the three-class approach. Three classifiers (RF, DT, and SVM) in the two-class approach achieved the best precision of 0.998.

Furthermore, the best recall was obtained by NN, RF, and DT in the three-classes approach, and by Bernoulli NB and Gaussian NB in both the three-class and two-class approaches. The best F1 score was obtained by LR in the two-stage approach, SVM in the three-class approach, and Bernoulli NB in the two-class approach. The highest F0.5 score was achieved by LR, SVM, and Bernoulli NB in the two-stage, three-class, and two-class approach, respectively. Furthermore, NN and DT achieved the best F2 score in the two-stage approach, SVM had the best F2 score in the three-class approach, and Bernoulli NB had the best F2 score in the two-class approach. Overall, Bernoulli NB with the two-class approach achieved the best F1, F0.5, and F2 scores.

6.4 Discussion

6.4.1 Principal Findings

The main purpose of this study was to identify and assess the effectiveness of AI methods and suitable health care staff–generated security practice data for measuring the security practice of health care staff in the context of big data. The main review findings are shown in Table 6.11. Eighteen studies met the inclusion and exclusion criteria. Recently, a related review for countermeasures against internal threats in health care also identified five machine learning methods that were fit for such measures [56]. This suggests that the adoption of AI methods for modeling and analyzing health care professional–generated security practice data is still an emerging topic of academic interest.

6.5 AI Methods

As shown in Tables 2 and 11, various algorithms were identified in the study, but the most used methods were KNN and NB algorithms. KNN is a supervised learning–based classification algorithm [1], which learns from labeled data. The KNN then tries to classify unlabeled data items based on the category of the majority of the most similar training data items known as K. The similarity between two data items in KNN can be determined according to the Euclidean distance of the various respective feature vectors of the data items [59]. NB is a probabilistic classifier algorithm based on the assumption that related pairs of features used for determining an outcome are independent of each other and equal [1]. There are two commonly used methods

Table 6.10: Malicious detection results using three approaches.

Classifier	Performance Measure	Two stage	Three classes	Two classes
Multinomial NBa				
	Precision	0.974	0.931	0.958
	Recall	0.752	0.802	0.831
	F1	0.849	0.862	0.89
	F0.5	0.92	0.902	0.93
	F2	0.788	0.825	0.854
Bernoulli NB				
	Precision	0.977	0.824	0.997
	Recall	0.832	0.881	0.881
	F1	0.898	0.852	0.935
	F0.5	0.944	0.835	0.971
	F2	0.857	0.869	0.902
Gaussian naive Bayes				
	Precision	0.977	0.695	0.994
	Recall	0.832	0.881	0.881
	F1	0.898	0.777	0.934
	F0.5	0.944	0.726	0.969
	F2	0.857	0.836	0.901
k-nearest neighbor				
	Precision	0.757	1	0.997
	Recall	0.832	0.703	0.702
	F1	0.792	0.826	0.824
	F0.5	0.771	0.922	0.92
	F2	0.816	0.747	0.746
neural network.				
	Precision	0.977	0.977	0.998
	Recall	0.842	0.851	0.851
	F1	0.904	0.91	0.919
	F0.5	0.947	0.949	0.965
	F2	0.866	0.874	0.877
logistic regression				
	Precision	1	0.966	0.998
	Recall	0.832	0.842	0.841
	F1	0.908	0.899	0.913
	F0.5	0.961	0.938	0.962
	F2	0.861	0.864	0.868
random forest				
	Precision	0.966	0.966	0.998
	Recall	0.842	0.832	0.831
	F1	0.899	0.894	0.907
	F0.5	0.938	0.935	0.959
	F2	0.864	0.855	0.86
decision tree.				
	Precision	0.977	0.954	0.998
	Recall	0.842	0.822	0.841
	F1	0.904	0.883	0.913
	F0.5	0.947	0.924	0.962
	F2	0.866	0.845	0.868
support vector machine				
	Precision	0.988	0.978	0.998
	Recall	0.832	0.861	0.861
	F1	0.903	0.916	0.924
	F0.5	0.952	0.952	0.967
	F2	0.859	0.882	0.885

Table 6.11: Principal findings of the review.

Category	Most used
Algorithms	KNN and Bayesian networks
Features	User IDs, patient IDs, device ID, date and time, location, route, and actions
Data sources	EHR and network logs
Security failures	Anomaly detection
Performance methods	True positive, false positive, false negative, ROCc curve, AUC
Data format	CVS
Nature of data sources	Real data logs
Ground truth	Similarity measures and observed data
Privacy preserving approaches	Tokenization and deidentification

of NB for classifying text: multivariant Bernoulli and multinomial models. KNN and NB algorithms have been more commonly used based on their comparatively higher detection accuracy. For instance, in an experimental assessment of KNN and NB for security countermeasures of internal threats in health care, both models showed over 90% accuracy with NB having a slight advantage over KNN (94% vs 93%). In a related study [56], the KNN method was found to have a higher detection rate with high TP rates and low FP rates.

The major issue with KNN in the context of health care staff security generated data is the lack of appropriate labeled data [68, 7, 21]. Within the health care setting, emergencies often dictate needs. In such situations, broader access to resources is normally allowed, making it challenging for reliable labeled data [68, 7, 21]. Therefore, in adopting KNN for empirical studies, the availability of appropriate labeled data should be considered; however, in the absence of labeled data, unsupervised clustering methods such as K-means clustering could also be considered [21].

6.5.1 Input Data

The input data that were mostly used in the reviewed studies include EHR logs and network data. Yeng et al [60] analyzed observational measures toward profiling health care staff security practices, and also identified various sources, including EHR logs, browser history, network logs, and patterns of keystroke dynamics [60]. Most EHR systems use an emergency access control mechanism known as "break-the-glass" or self-authorization" [4, 47]. This enables health care staff to access patients' medical records during emergency situations without passing through conventional procedures

for access authorization. A study [47] into access control methods in Norway revealed that approximately 50% of 100,000 patient records were accessed by 12,298 health care staff (representing approximately 45% of the users) through self-authorization. In such a scenario, EHR remains a vital source for analyzing deviations of required health care security practices.

Ground truth refers to the baseline, which is often used for training the algorithms [51]. The detection efficiency of the algorithms can be negatively impacted if the accuracy of the ground truth is low. As shown in Table 6.11, various methods—such as similarity measures, observed data, and historical methods—have been used. A similarity measure compares security practices with those of other health care professionals who have similar security practices. The observed measure is a control approach of obtaining the ground truth, whereby some users were observed to conduct their security practices under supervised, required settings [57]. However, the historical data have mainly relied on past records with a trust that the data are sufficiently reliable for the training set. These methods can be assessed for adoption in related studies.

6.5.2 Features and Data Format

EHRs contain most of the features that were identified in this review, as shown in Table 12.3. Features such as patient ID, actions, and user ID are primary features in EHR logs. The users' actions such as deletion, inserting, and updating, and various routes such as diagnosis, prescriptions, and drug dispensing can be tracked in EHR logs [47]. Guided with these findings, the simulated logs contained such attributes and features. Additionally, the simulation of the attributes of logs was also based on the security requirements of the EHRs of Norway [11, 60, 62, 61]. Eventually, a total of 21 attributes and 19 features were included in the simulated logs, as shown in Tables 6 and 7, respectively.

Security Failures and Privacy-Preserving Log Analysis The application of AI methods to analyze big data generated by health care professional security practice is a reactive approach. With such approaches, the primary aim is to determine deviations or outliers and maliciousness in health care security practices. Anomaly in this work refers to security practices in the access logs that deviate from established security and privacy policies in accessing patient records. For instance, health care workers could be required to access patient records if the health care staff is responsible for the patient throughout their shift and for therapeutic functions. However, it becomes abnormal if the health care staff access patient records outside of their shift. Additionally, if a patient's records are accessed when the patient has not registered for a visit to the hospital, this can also be considered abnormal. Furthermore, if health care staff are accessing patients' records more than usual, this also raises abnormal concerns, although some anomalous access could

be for therapeutic purposes and not with ill intentions. However, access that is not for therapeutic functions is described in this work as malicious. A greater proportion of the algorithms were applied for anomaly detection (67%). The detection of anomaly can clearly help in identifying the security practices that deviate from established security policies. However, Rostad and Edsberg [47] found that irregular access to patient records through self-authorization tended to be the normal security practice. An EHR system where a lot of access does not follow the established flow can make it unfeasible to manually track access with malicious intent [47]. Processing that incorporates the detection of malicious access, including intrusion detection, rather than merely detecting outliers could be an effective method of analyzing the security practice in the logs. Therefore, the identified 33% intrusion detections in the review were combined with maliciousness for the simulation since the outcome is to circumvent security requirement in both cases.

Privacy preservation in data mining provides a method to efficiently analyze data while shielding the identifications of the data subjects in a way that respects their right to privacy [2]. In the review, tokenization [8], deidentification [24], and removal of medical information [68] were some methods adopted to preserve privacy. The application of privacy-preserving methods in analyzing log data is crucial since health care data are classified among the most sensitive personal data [29]. Additionally, privacy-preserving methods need to be adopted in compliance with various regulations such as the General Data Protection Regulation [27]. Based on these findings from the review, a roadmap was drawn as a framework for empirical analysis of security practice in the big data context.

6.5.3 Research Implication and Practice

In this work, a comprehensive review was performed in security practice analysis, focusing on the use of AI methods to analyze logs of health care staff. Various AI algorithms, data sources, ground truth, features, application domain data file format, and nature of data sources were identified, analyzed, and modeled. To the best of our knowledge, this is the first time such a study has been systematically performed, along with development of a model and practical assessment of the model with simulated logs for future analysis with actual health care logs. In real log analysis, essential privacy measures such as tokenization and deidentification can be adopted.

Based on the review, a concept was established (Figure 12.3) on how data-driven and AI methods should be adopted to analyze the logs of EHRs in security practice. The concepts (two-stage, two-class, and three-class) were implemented and their performance was assessed with simulated logs. The attributes of the logs were comprehensive based on the review, which is another major contribution of this study. In the space of supervised learning,

our findings pinpoint the suitable algorithms and classification approaches that should be adopted for effective analysis of health care security practices.

Overall, the results of the simulation (Tables 9 and 10) showed that it is easier to differentiate between malicious and nonmalicious access than to distinguish between normal and nonmalicious abnormal access, which is mainly evident from the results of the two-stage approach. The performances of all classifiers in the second stage were far better than those in the first stage. This could also explain why the two-class approach was generally better than the two-stage and three-class approaches. Although the simulated data exhibited good performance with these methods, it is important to recognize that simulated data vary from real data; in particular, real data can be noisier and tend to have an adverse impact on a method's performance [34]. In the application of real data in this framework, effective preprocessing must be carried out toward reducing the noise and its related consequences.

6.5.4 Conclusion

Based on the galloping rate of data breaches in health care, HSPAMI was initiated to observe, model, and analyze health care staff security practices. One of the approaches in HSPAMI is the adoption of AI methods for modeling and analyzing health care staff–generated security practice data [60, 64]. This study was then performed to identify, assess, and analyze the appropriate AI methods and data sources. Out of 130 articles that were initially identified in the context of human-generated health care data for security measures in health care, 18 articles were found to meet the inclusion and exclusion criteria. After assessment and analysis, various methods such as KNN, NB, and DT were found to have been mainly applied on EHR logs with varying input features of health care staff security practices. A framework was therefore developed and practically assessed with simulated logs based on the review, toward analyzing real EHR logs.

Based on the results, for anomaly detection, DT algorithms obtained the best precision of 0.655, whereas the best recall was achieved by SVM at 0.977. However, the best F1-score was obtained by RF at 0.775. In brief, three classifiers (RF, DT, and SVM) in the two-class approach achieved the best precision of 0.998. Moreover, for malicious access detection, LR with the two-stage approach and KNN with the three-class approach obtained perfect precision (1.00), and the best recall was obtained by Bernoulli NB and Gaussian NB in both the three-class and two-class approaches with a value of 0.881. Furthermore, the best F1 score, F0.5 score, and F2 score for malicious access detection were achieved by Bernoulli NB using the two-class approach with values of 0.935, 0.971, and 0.902, respectively. These methods can therefore be used in analyzing health care security practice toward finding incentive measures for information security compliance in the health

care sector. This study covered only supervised learning where labeled data were used. Future work is therefore required using unsupervised learning methods in analyzing logs that do not have labeled data.

6.6 Bibliography

[1] ADEVA, J. J. G., AND ATXA, J. M. P. Intrusion detection in web applications using text mining. *Engineering Applications of Artificial Intelligence 20*, 4 (2007), 555–566. 170, 183

[2] AGRAWAL, R., AND SRIKANT, R. Privacy-preserving data mining. SIGMOD '00, Association for Computing Machinery, p. 439–450. Available from: https://doi.org/10.1145/342009.335438. 187

[3] AMÁLIO, N., AND SPANOUDAKIS, G. From monitoring templates to security monitoring and threat detection. In *2008 Second International Conference on Emerging Security Information, Systems and Technologies* (2008), IEEE, pp. 185–192. 170

[4] ARDAGNA, C. A., DI VIMERCATI, S. D. C., FORESTI, S., GRANDISON, T. W., JAJODIA, S., AND SAMARATI, P. Access control for smarter healthcare using policy spaces. *Computers & Security 29*, 8 (2010), 848–858. 160, 161, 185

[5] ASFAW, B., BEKELE, D., ESHETE, B., VILLAFIORITA, A., AND WELDEMARIAM, K. Host-based anomaly detection for pervasive medical systems. In *CRiSIS 2010, Proceedings of the Fifth International Conference on Risks and Security of Internet and Systems, Montreal, QC, Canada, October 10-13, 2010* (2010), IEEE Computer Society, pp. 1–8. 172

[6] BARO, E., DEGOUL, S., BEUSCART, R., AND CHAZARD, E. Toward a literature-driven definition of big data in healthcare. *BioMed research international 2015* (2015). 161

[7] BODDY, A., HURST, W., MACKAY, M., AND RHALIBI, A. E. A hybrid density-based outlier detection model for privacy in electronic patient record system, 2019. 170, 185

[8] BODDY, A. J., HURST, W., MACKAY, M., AND EL RHALIBI, A. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 170, 172, 187

[9] BOOTH, A., SUTTON, A., CLOWES, M., AND MARTYN-ST JAMES, M. Systematic approaches to a successful literature review. 166

[10] BÖSE, B., AVASARALA, B., TIRTHAPURA, S., CHUNG, Y.-Y., AND STEINER, D. Detecting insider threats using radish: A system for real-time anomaly detection in heterogeneous data streams. *IEEE Systems Journal 11*, 2 (2017), 471–482. 164, 165

[11] CANNOY, S. D., AND SALAM, A. A framework for health care information assurance policy and compliance. *Communications of the ACM 53*, 3 (2010), 126–131. 162, 164, 186

[12] CHANDRA, S., RAY, S., AND GOSWAMI, R. Big data security in healthcare: survey on frameworks and algorithms. In *2017 IEEE 7th International Advance Computing Conference (IACC)* (2017), IEEE, pp. 89–94. 164

[13] CHEN, Y., AND MALIN, B. Detection of anomalous insiders in collaborative environments via relational analysis of access logs. In *Proceedings of the first ACM conference on Data and application security and privacy* (2011), pp. 63–74. 170

[14] CHEN, Y., NYEMBA, S., AND MALIN, B. Detecting anomalous insiders in collaborative information systems. *IEEE transactions on dependable and secure computing 9*, 3 (2012), 332–344. 170

[15] CHEN, Y., NYEMBA, S., ZHANG, W., AND MALIN, B. Specializing network analysis to detect anomalous insider actions. *Security informatics 1*, 1 (2012), 1–24. 164, 165

[16] COSTANTE, E., FAURI, D., ETALLE, S., DEN HARTOG, J., AND ZANNONE, N. A hybrid framework for data loss prevention and detection. In *2016 IEEE Security and Privacy Workshops (SPW)* (2016), IEEE, pp. 324–333. 170, 172

[17] FAUZI, M. A., AND BOURS, P. Ensemble method for sexual predators identification in online chats. In *2020 8th International Workshop on Biometrics and Forensics (IWBF)* (2020), pp. 1–6. 179

[18] FOR EHEALTH", D. The code of conduct for information security and data protection in the healthcare and care services, 2020. Available from: "`https://www.ehelse.no/normen/documents-in-english`". 160, 161

[19] GAFNY, M., SHABTAI, A., ROKACH, L., AND ELOVICI, Y. Detecting data misuse by applying context-based data linkage. In *Proceedings of the 2010 ACM workshop on Insider threats* (2010), pp. 3–12. 164, 165

[20] GARRITY, M. Patient medical records sell for $1k on dark web, 2019. Available from: `https://`

www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.htmlhttps://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html. 161

[21] GATES, C. S., LI, N., XU, Z., CHARI, S. N., MOLLOY, I., AND PARK, Y. Detecting insider information theft using features from file access logs. In *Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II* (2014), M. Kutylowski and J. Vaidya, Eds., vol. 8713 of *Lecture Notes in Computer Science*, Springer, pp. 383–400. Available from: https://doi.org/10.1007/978-3-319-11212-1_22. 185

[22] GDPR. Implementation of gdpr in health care sector in norway, 2019. Available from: https://ehelse.no/personvern-og-informasjonssikkerhet/eus-personvernforordning/implementation-of-gdpr-in-health-care-sector-in-norway. 178

[23] GHEYAS, I. A., AND ABDALLAH, A. E. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big data analytics 1*, 1 (2016), 1–29. 164

[24] GUPTA, S., HANSON, C., GUNTER, C. A., FRANK, M., LIEBOVITZ, D., AND MALIN, B. Modeling and detecting anomalous topic access. In *2013 IEEE International Conference on Intelligence and Security Informatics* (2013), IEEE, pp. 100–105. 170, 172, 187

[25] HOLMES, J., SACCHI, L., BELLAZZI, R., ET AL. Artificial intelligence in medicine. *Ann R Coll Surg Engl 86* (2004), 334–8. 161, 163

[26] HUMER, C., AND FINKLE, J. Your medical record is worth more to hackers than your credit card. *Reuters. com US Edition 24* (2014). 161

[27] IMPERVA. Pseudonymization, 2020. Available from: https://www.imperva.com/data-security/compliance-101/pseudonymization/. 187

[28] ISLAM, M. S., HASAN, M. M., WANG, X., GERMACK, H. D., AND NOOR-E-ALAM, M. A systematic review on healthcare analytics: application and theoretical perspective of data mining. In *Healthcare* (2018), vol. 6, MDPI, p. 54. 164, 165

[29] ISO. Health informatics information security management in health using iso/iec 27002, 2016. Available from: "https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en". 187

[30] JIANG, F., JIANG, Y., ZHI, H., DONG, Y., LI, H., MA, S., WANG, Y., DONG, Q., SHEN, H., AND WANG, Y. Artificial intelligence in healthcare: past, present and future. *Stroke and vascular neurology 2*, 4 (2017). 163

[31] KHAN, R. A., AND KHAN, S. U. A preliminary structure of software security assurance model. In *Proceedings of the 13th International Conference on Global Software Engineering* (2018), pp. 137–140. 166

[32] KHRAISAT, A., GONDAL, I., VAMPLEW, P., AND KAMRUZZAMAN, J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity 2*, 1 (2019), 1–22. 164

[33] KITCHENHAM, B., PRETORIUS, R., BUDGEN, D., BRERETON, O. P., TURNER, M., NIAZI, M., AND LINKMAN, S. Systematic literature reviews in software engineering–a tertiary study. *Information and software technology 52*, 8 (2010), 792–805. 166

[34] KONONENKO, I., AND KUKAR, M. *Machine learning and data mining*. Horwood Publishing, 2007. 163, 172, 188

[35] KWON, J., AND JOHNSON, M. E. The market effect of healthcare security: Do patients care about data breaches? In *WEIS* (2015). 162

[36] LI, X., XUE, Y., AND MALIN, B. Detecting anomalous user behaviors in workflow-driven web applications. In *2012 IEEE 31st Symposium on Reliable Distributed Systems* (2012), IEEE, pp. 1–10. 170

[37] MCLEOD, A., AND DOLEZEL, D. Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems 108* (2018), 57–68. 162

[38] MCLEOD, A., AND DOLEZEL, D. Understanding healthcare data breaches: Crafting security profiles. 162

[39] MENON, A. K., JIANG, X., KIM, J., VAIDYA, J., AND OHNO-MACHADO, L. Detecting inappropriate access to electronic health records using collaborative filtering. *Machine learning 95*, 1 (2014), 87–101. 170

[40] NIST. Verizon data breach investigations report, 2019. Available from: `https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf`. 161

[41] NWEKE, L. O., YENG, P., WOLTHUSEN, S., AND YANG, B. Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices. 161, 162

[42] PETERSEN, K., VAKKALANKA, S., AND KUZNIARZ, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology 64* (2015), 1–18. 166

[43] PIERROT, D., HARBI, N., AND DARMONT, J. Hybrid intrusion detection in information systems. In *2016 International Conference on Information Science and Security (ICISS)* (2016), IEEE, pp. 1–5. 170

[44] PREDD, J., PFLEEGER, S. L., HUNKER, J., AND BULFORD, C. Insiders behaving badly. *IEEE Security & Privacy 6*, 4 (2008), 66–70. 162

[45] PRISMA. Prisma, 2018. Available from: `http://www.prisma-statement.org/`. 167

[46] RIGGS, C. *Network perimeter security: building defense in-depth*. Auerbach Publications, 2003. 162

[47] ROSTAD, L., AND EDSBERG, O. A study of access control requirements for healthcare systems based on audit trails from access logs. In *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)* (2006), IEEE, pp. 175–186. 160, 161, 162, 175, 185, 186, 187

[48] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 162

[49] SHABAN-NEJAD, A., MICHALOWSKI, M., AND BUCKERIDGE, D. L. Health intelligence: how artificial intelligence transforms population and personalized health, 2018. 163

[50] SIRAJ, A., VAUGHN, R. B., AND BRIDGES, S. M. Decision making for network health assessment in an intelligent intrusion detection system architecture. *Int. J. Inf. Technol. Decis. Mak. 3*, 2 (2004), 281–306. 170

[51] SMYTH, P., FAYYAD, U. M., BURL, M. C., PERONA, P., AND BALDI, P. Inferring ground truth from subjective labelling of venus images. In *Advances in Neural Information Processing Systems 7, [NIPS Conference, Denver, Colorado, USA, 1994]* (1994), G. Tesauro, D. S. Touretzky, and T. K. Leen, Eds., MIT Press, pp. 1085–1092. 186

[52] T., T. Hackers, breaches, and the value of healthcare data., 2019. Available from: `https://www.securelink.com/blog/healthcare-data-new-prize-hackers/`. 161

[53] TCHAKOUCHT, T. A., EZZIYYANI, M., JBILOU, M., AND SALAUN, M. Behavioral appraoch for intrusion detection. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)* (2015), IEEE, pp. 1–5. 172

[54] VIHINEN, M., AND SAMARGHITEAN, C. Medical expert systems. *Current Bioinformatics 3*, 1 (2008), 56–65. 163

[55] WAHL, B., COSSY-GANTNER, A., GERMANN, S., AND SCHWALBE, N. R. Artificial intelligence (ai) and global health: how can ai contribute to health in resource-poor settings? *BMJ global health 3*, 4 (2018), e000798. 163

[56] WALKER-ROBERTS, S., HAMMOUDEH, M., AND DEHGHANTANHA, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access 6* (2018), 25167–25177. 164, 165, 183, 185

[57] WESOŁOWSKI, T. E., PORWIK, P., AND DOROZ, R. Electronic health record security based on ensemble classification of keystroke dynamics. *Applied Artificial Intelligence 30*, 6 (2016), 521–540. 170, 186

[58] WHITMAN, M. E., FENDLER, P., CAYLOR, J., AND BAKER, D. Rebuilding the human firewall. In *Proceedings of the 2nd annual conference on Information security curriculum development* (2005), pp. 104–106. 162

[59] YENG, P., WOLDAREGAY, A. Z., AND HARTVIGSEN, G. K-cusum: Cluster detection mechanism in edmon. 183

[60] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 160, 161, 162, 164, 185, 186, 188

[61] YENG, P. K., FAUZI, M. A., AND YANG, B. Comparative analysis of machine learning methods for analyzing security practice in electronic health records' logs. In *2020 IEEE International Conference on Big Data (Big Data)* (2020), IEEE, pp. 3856–3866. 186

[62] YENG, P. K., FAUZI, M. A., AND YANG, B. Workflow-based anomaly detection using machine learning on electronic health records' logs: A comparative study. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)* (2020), IEEE, pp. 753–760. 186

[63] YENG, P. K., NWEKE, L. O., WOLDAREGAY, A. Z., YANG, B., AND SNEKKENES, E. A. Data-driven and artificial intelligence (ai) approach for modelling and analyzing healthcare security practice: a systematic review. In *Proceedings of SAI Intelligent Systems Conference* (2020), Springer, pp. 1–18. 165

[64] YENG, P. K., SZEKERES, A., YANG, B., AND SNEKKENES, E. A. Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: Systematic mapping study. *JMIR human factors 8*, 2 (2021), e17604. 162, 188

[65] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 161, 162, 163, 165

[66] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 163, 165

[67] ZHANG, H., MEHOTRA, S., LIEBOVITZ, D., GUNTER, C. A., AND MALIN, B. Mining deviations from patient care pathways via electronic medical record system audits. *ACM Transactions on Management Information Systems (TMIS) 4*, 4 (2013), 1–20. 170

[68] ZIEMNIAK, T. Use of machine learning classification techniques to detect atypical behavior in medical applications. In *2011 Sixth International Conference on IT Security Incident Management and IT Forensics* (2011), IEEE, pp. 149–162. 163, 170, 172, 185, 187

IEEE BigData 2020 2020 IEEE International Conference on Big Data; https://doi.org/10.1109/BigData50022.2020.9378353

Chapter 7

Comparative analysis of machine learning methods for analyzing security practice in electronic health records' logs.

2020 IEEE International Conference on Big Data (Big Data)

Prosper K. Yeng, Muhammad A. Fauzi, and Bian Yang

Abstract

Electronic health records (EHR) consists of broad, numerous and erratic accesses through self-authorizations and "brake the glass" scenarios. This is to fulfil the availability aspect of the the CIA (confidentiality, integrity) due to the time sensitive nature in healthcare especially during health emergency situations. Adversaries can use this as opportunity to illegitimately access patients records, thereby, compromising the entire EHR system. To avert this, a comparative analysis of machine learning classification methods was conducted with simulated EHR logs. The methods which were compared are Multinomial Naive Bayes(multnb), Bernoulli Naive Bayes (bernnb), Support Vector Machine (svm), Neural Network (nn), K-Nearest Neighbours(knn), Logistic Regression (lr), Random Forest (rf), and Decision Tree (dt).

The experiment results show that all of the machine learning models used in this work performed very well for the role classification task but, Decision Tree (dt) and Random Forrest (rf) obtained the best result among all of the methods with the same accuracy value of 0.889 on all three datasets. For the anomaly detection task, generally, our proposed approach obtained a high recall and accuracy but low precision and F1-score. Soft Classification approach performed better than the Hard Classification approach. The best performance was achieved with Bernoulli Naive Bayes with none normalised data, with an F1-score of 0.893.

7.1 Introduction

Undermining required information security practice is in fact, a paradox to healthcare's objective. Healthcare professionals and major stakeholders (governments, non-governments, cares, and love ones) do put in all their efforts to save the lives of their subjects of care. In that vein, information systems are being relied on in recent times by hospitals to obtain better efficiency. This demands for the adoption of appropriate security measures (otherwise called required security practice) by the healthcare staff. Intentional or unintentional negligence in observing these required security practices tend to reverse the efforts of healthcare on patients' care since the sensitive patient records can be compromised. For instance, in a recent ransomware attack at Duesseldorf University Clinic in Germany, the medical records of a patient were not timely available during emergency and this resulted in the death of that patient [1].

Sound security practice involves all categories of the information systems' users who form the healthcare staff (including the healthcare professionals who provide therapeutic care and paramedical staffs such as health administrators, IT administrators, human resource personnel and finance) to follow laid down standards, policies, procedures, guidelines and code of conduct in the usage of the information systems in order to avoid compromising the confidentiality, integrity and availability (CIA) of the systems.

Good security practice is so much needed in healthcare because the healthcare data is classified as one of the most sensitive personal information [16] which is faced with multifaceted threats. Such threats are masquerades (insiders, service providers, outsiders), communication interference, repudiation, misuse of system resources, system failures or errors, theft, damaging of resources and unauthorised access. Meanwhile, the healthcare systems are exposed to many users including their subjects of care, the healthcare professionals, contracted IT staff and locum personnel who are the weakest link in the security chain.

The critical importance in healthcare requires the sector to collect detailed patients information to enable them to correctly identify each patient and correctly map each patient to their medical records. This results in a collection of huge sensitive personal data which is of great importance to cyber criminals who can use it to commit multiple harm including identity theft [16].

Therefore, technological measures have since been the default and traditional approach in protecting these records. But these technical measures are being circumvented by the adversaries through the frequent manipulation of the healthcare workers to compromise these records. Due to the difficulties for cybercriminals to directly overcome the perimeters of technical security solutions, the healthcare workers are often masqueraded through social engineering attacks and other human related means of attack to gain

unauthorised access. Insider intentional or unintentional security malpractice also tend to cause data breaches which can course serious harm to the patients.

In 2017, the healthcare sector in the United Kingdom had a bad experience with the wannacry ransomware which affected critical care [7, 12], spread to about 150 countries and affected about 230,000 computers in different sectors. Subsequently, about 3 million healthcare records were compromised in Norway in 2018[32, 30] of which an insider aid was involved. Additionally, there was another phishing attack which resulted in compromising about 38,000 patient records in Portland, Oregon-based Legacy Health in the United States in 2019 [26]. The personal data which was comprised includes patients' email accounts, demographic information, dates of birth, health insurance data, billing details, medical data, Social Security numbers, and driver's licenses numbers. Healthcare data breaches continue to surge, with the passage of time. Globally, about 5 million healthcare records were compromised in 2017, followed by 15 million records in 2018 and 25 million records as at the middle of 2019[27]. Quite recently, Universal Health Services (UHS), which is operating about 400 health facilities, was massively attacked with a ransomware and this was believed to possibly be the largest security incident in healthcare in the US [13]. The impact has led to a multiday offline IT network across UHS facilities throughout the country. Information security incidents are threatening the quality of healthcare [5] delivery of which the information technology was rather to improve. -what are the possible causes of these attacks in the context of the human elements? *Many bad actors use malicious emails, malspam and social engineering to make their way into the network, while some rely on exploiting vulnerabilities on Internet-facing devices.

As the saying goes that "an unexamined life is not worthy living", there is hence the need to assess the way of life of security practice of the human elements towards controlling these data breaches in healthcare. Good security practices have been defined in regulations, policies, standards, guidelines and code of conducts which are required to be implemented with both technical and non-technical measures. Technical security measures including firewalls, intrusion detection, and prevention have been fortified over time because they have since been the default and traditional security countermeasures. The challenging part is the human elements in the security chain who are the weakest link of which hackers mostly use in recent time to complete their attack.

In contributing to the fight against cyber attacks in healthcare, there is the need to understand the extend of users' compliance with the established security policies.For instance What are the challenges often faced by the healthcare workers in their effort to comply with these required security practices while doing their work? Are these security measures conflicting

with the healthcare worker? How can the required security practices be improved for effective compliance while improving security effectiveness? How can the healthcare workers be incentivized to better comply with required security practice admist their work? Or which required security measures need to be modified to enhance effective compliance?

In efforts towards answering these questions effectively, there is the need to analyze healthcare information security practice in the human context by looking for the gaps that exist between current healthcare workers' security practice and their required security practice which are defined in the legislation, regulations, standards, policies, guidelines, procedures, best practices and code of conducts [30].

- What are the various ways of analyzing security practice and one of them is the EHR logs

There exists various ways in which security practices can be analysed. One of them is the modeling and analysing of the psychological, social, cultural and demographic perspectives of the healthcare workers' security practice [31]. This can be achieved by gathering and analyzing data on knowledge, attitude, opinion, behaviour, facts, etc., on the healthcare workers', objects, and events in a research survey [23, 22, 31, 30, 5, 15, 25, 8]. Another dimension involves analysing the social engineering behavior of the healthcare workers to determine their ability to identify and avoid such related attacks. [28, 9, 10]. Additionally, since the healthcare workers often access various assets and resources (eg healthcare records, physical access, networks etc) while leaving traces of their accesses which that can be reconstructed into their unique profile, there is the need to model and analyze the access logs of healthcare workers to understand their security practice in the aspect of big data [2, 3, 6].

Identified dilemmas can then be resolved with appropriate measures by devising means of resolving the challenges and providing incentivization methods for enhanced security practice. While all these approaches are important, the focus of this paper is to analyze healthcare security behaviour in the context of big data in relation to logs of electronic healthcare records.

Yeng et al identified network logs, EHR logs, keystroke dynamics and host based logs as some of the data sources which are being used for modeling and analyzing healthcare security practices [33]. Among these data sources, EHR logs was mostly used in the context of data-driven and AI approach. According to Boddy et al, EHR is one of the cardinal assets in the healthcare infrastructure which should be proactively monitored to detect both internal and external threats. To detect anomaly activities such as medical record snooping, social engineering threats to acquire healthcare professionals' logon credentials, erratic or unusual activities, there is the need to consider the modeling and analyzing of EHR [3, 34].

Due to emergency situations and the time sensitive nature of health-

care, there is usually the provision of a broad access to patients' healthcare records by the healthcare professionals in a typical hospital. In a role-based access control scenario, the healthcare workers in their assigned roles need to have similar pattern of access to patient records. For instance, the behaviour of users with nursing role should be similar in their accesses. However, if a nurse accesses within a period, tend to deviate from nursing role, then an abnormally can be quarried. Similarly, if an IT officers' role tend to act like a medical doctor within a given time, then an anomaly flag need to be raised. Inference can therefore be conducted into the anomalies to determine their maliciousness.

7.1.1 Related work

Various related studies have been conducted to safeguard electronic health records through the detection of anomalies in electron health records.For instance, [3] employed density-based local outlier detection model to profile users activities and their respective interactions with devices to detect and visualized abnormal security practices.A local outlier detection factor (LOF) assessed the local deviation of density by measuring the isolated distance of a data point to its k-nearest neighbours. Out of an unlabeled data set of 1,007,727 audit logs, the algorithm detected 144 anomalous behaviours. Also, a prediction method, dyadic prediction, [14] with collaborative filtering techniques was adopted by [21]. This method was used to predict the interaction of entity pairs just like how friends are recommended in social network, click-through rate prediction in computational advertising[20] and the prediction of the performance of students' test scores. The collaborative principle is about the assumption that if a person A and a person B share the same opinion on an issue, it is highly probable that the pair will have the same opinion in a different issue either than a randomly selected different person [20]. Additionally, Ziemniak et al employed C4.5 decision tree to detect abnormal security practice in a healthcare application. Ad-hoc analyis was used to determine atypical behaviour by visually looking for interesting nodes such as path-length investigation [34]. Furthermore, Gupta et al used K- Nearest Nieghbor (KNN) algorithm for the detection of outliers with the goal to detect anomalous users. Random topic access model (RTA) was targeted to identify users with illegitimate accesses with focus on common semantic themes [11]. Latent Dirichlet Allocation (LDA) was adopted in this study as a feature extraction technique. All these studies[3, 14, 20, 11] adopted various machine learning methods in their work however, a comparative analysis was not conducted to guide in the selection of the methods.

Healthcare data logs consists of various roles in which different roles can have close similarities in their operations. Additionally, there are erratic accesses due to uncertainties in healthcare such as emergency situations[24, 33]. For instance, healthcare systems have an emergency access mechanism

known as "break the glass" or self-authorization which enables healthcare workers to access patients records without following the conventional authorization process[24, 33]. This opens up the system for numerous accesses in which various difference accesses can be similar[24, 33]. For instance, how will nurse A activities be distinguished from doctor A's activities in which both provided diagnosis and prescription to patients? Therefore, in analysing security practice in healthcare, it is necessary to compare the algorithms to determine the method that is fit for the purpose.

In that light, [19] compared Hidden markov model(HMM) and Distance-based model towards detecting anomalous user behaviours based on the sequence of their accesses within web sessions of electronic health application. The web sessions of users were converted into their respective workflows based on their respective access targets. So the anomalous workflows of users were being detected as their respective abnormal behaviours. Additionally, [6] compared community-based anomaly detection system wtih K-nerarset neighbors(KNN) and principal component analysis towards detecting threats in EHR based on the access logs of the healthcare staff. In the study, CAD performed better than KNN and PCA in Area under the ROC curve (AUC). Two methods each were compared in these studies([19, 6] to enable the selection of a better algorithm. However, there a other classification methods such as decision trees and rules, Bayesian classifiers, nearest neighbor classifiers, discriminant functions, support vector machines and neural networks [18] which were not considered in their studies.

7.1.2 Scope and contribution

Based on the gaps in the related works and review [33], we simulated electronic health records logs to perform the comparative analysis of the machine learning classification algorithms towards analyzing healthcare security practice. Aside the comparative analysis, various approaches called hard and soft classifications were performed and compared. The hard classification computed for the probabilities of each daily accumulated activities and classified the most probable into the respective role. But, the soft classification adopted a thresh holding mechanism. So if the probability of accumulated daily activities of a user meets a given threshold, that activity is then assigned into the given role. Furthermore, we compared the performance of z-score and Min-max normalization methods to access the performance of the algorithms in that aspect.

7.2 Our Method

7.2.1 Health record logs data simulation

We simulated a one-year access log data of the hospital information system from 01 January 2019 until 31 December 2019. We simulated five main modules in the hospital information system: Report, Finance, Patient Management, Laboratory Management, and Pharmacy Management. In the data simulation setting, we use 19 departments and 12 roles as displayed in Table 7.1 and Table 7.2. There are two kinds of shifts used: the regular shift and the three 8 hours shift. The regular shift is from Monday to Friday 08.00-16.00 while the three 8 hours shift contains three shifts every day: a) Shift 1: 06.00-14.00, b) Shift 2: 14.00-22.00, and c) Shift 3: 22.00-06.00 (next day). The number of roles and employees in a regular shift can be seen in Table 8.1 while that in three 8-hours shifts can be seen in Table 8.2.

Table 7.1: List of Departments

ID	Name
0	IT
1	Finance
2	Administration
3	Laboratory
4	Pharmacy
5	Out Patients Ear-Nose-Throat
6	Out Patients Eyes
7	Out Patients Tooth
8	Out Patients Child
9	Out Patients Orthopedic
10	Out Patients Neurological
11	Out Patients Gynecological
12	Out Patients Diabetes
13	Out Patients Rheumatology
14	Out Patients Cancer
15	Emergency
16	In Patients Ward1
17	In Patients Ward2
18	In Patients Ward3

In this simulation, the flow of patients in the inpatients, outpatients, and emergency department are displayed in Fig. 8.1, 8.2, and 8.3 respectively. Based on the flows, we simulated the data and recorded the logs. The logs is considered as normal data (non anomaly). Besides, we also simulate some abnormal data. The abnormal data are generated by simulating attackers

Table 7.2: List of Roles

ID	Name	Code
0	Head of IT	HIT
1	Technical Support	TS
2	Head of Finance	HF
3	Finance Staff	FS
4	Head of Administration	HA
5	Staff of Administration	SA
6	Head of Lab	HL
7	Lab Assistant	LA
8	Head of Pharmachy	HP
9	Pharmacy Assistant	PA
10	Doctor	DO
11	Nurse	NU

Table 7.3: Regular Shift

ID	Department	Roles (number of employees)
0	IT	HIT(1), TS(2)
1	Finance	HF(1), FS(4)
2	Administration	HA(1), SA(2)
3	Laboratory	HL(1), LA(5)
4	Pharmacy	HP(1), PA(2)
5	Out Patients Ear-Nose-Throat	DO(1), NU(2)
6	Out Patients Eyes	DO(1), NU(2)
7	Out Patients Tooth	DO(1), NU(2)
8	Out Patients Child	DO(1), NU(2)
9	Out Patients Orthopedic	DO(1), NU(2)
10	Out Patients Neurological	DO(1), NU(2)
11	Out Patients Gynecological	DO(1), NU(2)
12	Out Patients Diabetes	DO(1), NU(2)
13	Out Patients Rheumatology	DO(1), NU(2)
14	Out Patients Cancer	DO(1), NU(2)
16	In Patients Ward1	DO(1)
17	In Patients Ward2	DO(1)
18	In Patients Ward3	DO(1)

that are assumed have compromised some users credential and use it to access patients records (e.g. identity theft). The attacker will access more data than legitimate users and sometimes not follow the flows. From this data simulation, 283.678 logs were created with 274.983 of them are legitimate access while 8.695 of them are fraudulent. There are 21 fields recorded in this data simulation like displayed in Table 8.3.

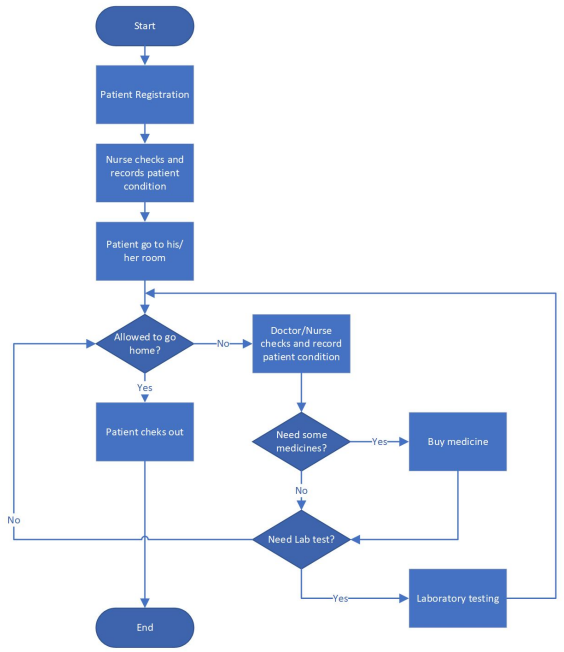


Figure 7.1: The Inpatients Department Flow

Table 7.4: Three 8-hours shift

ID	Department	Roles (number of employees)
15	Emergency	DO(2), NU(7)
16	In Patients Ward1	NU(2)
17	In Patients Ward2	NU(2)
18	In Patients Ward3	NU(2)

Table 7.5: Record Fields

#	Field Name	Description
1	startAccessTime	The time employee start to acces the patient record. format = 'dd/mm/yyy HH:mm tt'
2	endAccessTime	The time employee end the patient record access. format = 'dd/mm/yyy HH:mm tt'
3	employeeID	The ID of the employee who access the patient record
4	roleID	The role of the employee who access the patient record
5	patientID	The ID of the patient whose record is being accessed by employee
6	activityID	The ID of the activity (1: Create, 2: Read, 3:Update, 4: Delete)
7	employee DepartmentID	The department of the employee who access the patient record
8	employee OrganizationID	The organization of the employee who access the patient record
9	osID	The OS of the computer used by the employee to access patient record
10	deviceID	The ID of the computer used by the employee to access patient record
11	browserID	The browser used by the employee to access patient record
12	ipAddress	The IP Address of the computer used by the employee to access patient record
13	ReasonID	The reason of employee access the patient record (optional)
14	shiftID	The ID of shift the employee belong to on the day of patient access record
15	siftStart DateTime	The start time of shift the employee belong to on the day of patient access record
16	siftEnd DateTime	The end time of shift the employee belong to on the day of patient access record
17	CRUD	The ID of the activity (C: Create, R: Read, U:Update, D: Delete)
18	Access ControlStatus	Access Control Status
19	SessionID	The ID of the session access
20	AccessPatient_Warnings	Warning for not usual access
21	ModuleUsed	The module acessed by the employee

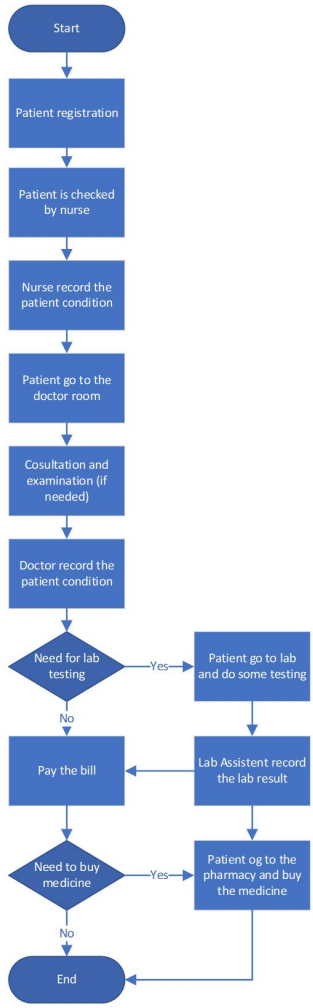


Figure 7.2: The Outpatients Department Flow

7.2.2 Proposed method for anomaly detection

The anomaly detection method used is based on the fact that people with the same role have similar activities and people with different roles tend to have different activities. For example, Doctor A and Doctor B tend to have similar activities but Doctor A and IT staff C are unlikely to have similar activities. If Doctor A's activity on a particular day has a low similarity with

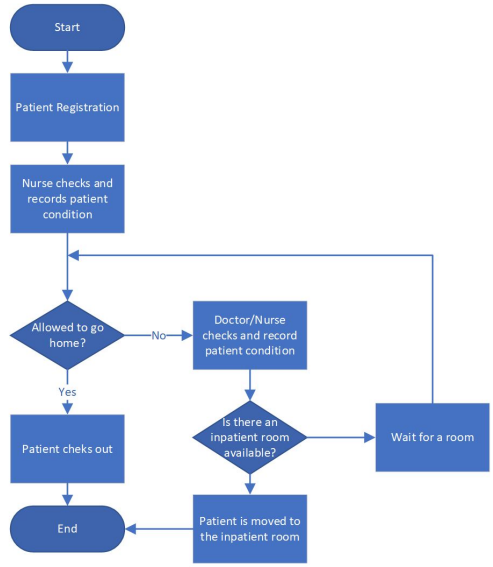


Figure 7.3: The Emergency Department Flow

doctor's activity but has a high similarity with the IT staff's activity, then the Doctor A's activity on that particular day can be abnormal.

The method proposed in this work aims to identify the anomaly by comparing the user's activity to their role's normal activity, such as the type of actions being taken and the number of patients they are viewing. First, a model for role classification is trained. Then, using the model, the activity of each user is classified. If the activity is classified into the real role of the user, the activity is considered normal. Otherwise, the activity is considered an anomaly. In this way, potentially illegitimate access to patient records can be highlighted and investigated.

7.2.2.1 Feature Extraction

To develop the anomaly detection model, including the role classification model, some features were extracted. Each log entry represents a single transaction for a user. To analyze the user activity, the logs from each user are consolidated into a particular period. Every single activity of Doctor A is a poor data point that will be hard to analyze separately. However, by observing several activities of Doctor A for a particular period, it will be easier to do the anomaly detection task. In this work, we process the logs data into 24-hour blocks so that an instance represents the cumulative

activity of a user in a single day. As the results, 24,648 instances are extracted from the raw logs with 24,286 of them are considered normal and 362 of them are considered an anomaly. The definition of anomaly data here is all the instances had at least one fraudulent log access in a single day while the normal data are all the instances whose all access logs are in line with the roles. Afterward, these instances are then transformed into features for role classification and anomaly detection processes. Table 9.6 shows the features extracted from the dataset. In this work, we also use two normalization methods: Z-score normalization, and Min-Max normalization.

7.2.2.2 Role Classification Model

Since the anomaly detection method in this work is based on the role classification, we need to build the role classification model first. The goal of role classification is to classify the cumulative user activity in a single day into one of the 12 categories as shown in 7.2 . The model is trained using only normal data because the anomaly data are data from the attacker that tend to behave differently from the real users. Then, the model is used to classify the cumulative activity of a user in a single day. Eight machine learning methods were used as classifiers for the role classification model including Multinomial Naive Bayes(multnb), Bernoulli Naive Bayes (bernnb), Support Vector Machine (svm), Neural Network (nn), K-Nearest Neighbours(knn), Logistic Regression (lr), Random Forest (rf), and Decision Tree (dt). To evaluate the model, we conducted 5-folds cross-validation on the normal data. The number of normal data is 24,286 instances. The evaluation method for this task is accuracy.

7.2.2.3 Anomaly Detection

The anomaly detection method used in this work is based on the role classification model. There are two different approaches employed as follows:

- Hard Classification: In this approach, we classify each instance (cumulative user activity in a single day) into one category. Like mentioned before, the categories used are the list of roles in the hospitals. Since there are 12 roles in the simulated hospital, the number of categories is also 12. If the user's cumulative activity in a single day is classified into her/his actual role, then the instance is considered normal. Otherwise, if the user's cumulative activity in a single day is not classified into her/his actual role, then the instance is considered an anomaly. For example, if Doctor A's cumulative activity in a single day is classified into the Doctor category, then it is considered normal. Otherwise, if Doctor A's cumulative activity in a single day is classified into other categories than Doctor (e.g. Nurse, Technical Support, etc.), then it is considered an anomaly.

Table 7.6: Dataset feature names and descriptions

Feature Name	**Description**
number of create	Number of 'create' transactions conducted in a single day
number of read	Number of 'read' transactions conducted in a single day
number of update	Number of 'update' transactions conducted in a single day
number of delete	Number of 'delete' transactions conducted in a single day
number of patient record	Number of access to the patient records in a single day
number of unique patient	Number of unique patients whose records has been accessed in a single day
number of modules	Number of kind of modules in the information system accessed in a single day
number of report module	Number of transactions conducted in the report module in a single day
number of finance module	Number of transactions conducted in the finance module in a single day
number of patient module	Number of transactions conducted in the patient management module in a single day
number of lab module	Number of transactions conducted in the laboratory module in a single day
number of pharmacy module	Number of transactions conducted in the pharmacy module in a single day
number of outside access	Number of transactions conducted from outside hospital network in a single day
number of browser	Number of browser type used in a single day
number of chrome	Number of chrome browser used in a single day
number of ie	Number of Internet Explorer browser used in a single day
number of safari	Number of Safari browser used in a single day
number of firefox	Number of Firefox browser used in a single day
number of other browser	Number of other browser used in a single day

- Soft Classification: This approach is similar to the hard classification approach but in a softer way. It gives tolerance for the user to act like users from other roles because some roles have quite similar activities. In this approach, the classifier computed the probability of the user's instance belong to their role class. If the probability is above a particular threshold, then it is considered normal. Otherwise, it will be considered an anomaly. For example, the classifier will compute the probability of Doctor A's cumulative activity in a single day into the Doctor category because his actual role is Doctor. Then, if the probability is above a particular threshold, then it is considered normal. Otherwise, it will be considered an anomaly.

To evaluate this anomaly detection, we use the logs from January until August as training data while data from September until December is used for testing data. The training data is used to train the role classification model. Then, this model is used to detect anomaly based on the two proposed approaches. For this task, precision, recall, and f1-measure are used to evaluate the method.

7.2.3 Performance Evaluation

For the role classification task, accuracy is used for evaluation. The following is the formula to calculate the accuracy:

$$Accuracy = \frac{NumberOfCorrectPrediction}{NumberOfData} \tag{7.1}$$

where $NumberOfCorrectPrediction$ is the number of instances that are correctly classified into their actual role while $NumberOfData$ is the total number of instances in the dataset.

		Predicted	
		Anomaly	Normal
Actual	Anomaly	TP	FN
	Normal	FP	TN

Figure 7.4: Confusion Matrix

For the anomaly detection, several measurements including Accuracy (Acc), Precision (P), Recall (R), and F_1-score (F_1) were used to evaluate the performance. All measurements were calculated based on the confusion matrix displayed in Fig. 8.4. True Positive (TP) and True Negative (TN) are the numbers of features that were correctly predicted. TP represents

the number of anomaly data that were correctly predicted as an anomaly while TN represents the number of normal data or users that were correctly predicted as normal. Meanwhile, False Positive (FP), or often called Type I Error is the number of normal data that were incorrectly predicted as anomaly ones and False Negative (FN) or Type II Error represents the number of anomaly data that were incorrectly predicted as normal ones. The followings are the formulas for each measurement:

$$Acc = \frac{TP + TN}{TP + FP + FN + TN} \tag{7.2}$$

$$P = \frac{TP}{TP + FP} \tag{7.3}$$

$$R = \frac{TP}{TP + FN} \tag{7.4}$$

$$F_1 = 2\frac{P \cdot R}{P + R} \tag{7.5}$$

7.3 Result

7.3.1 Role Classification Model Result

The experiment result of the role classification model is depicted in Table 7.7. Overall, all of the machine learning method employed shows a good performance with an accuracy of more than 0.7. Decision Tree (dt) and Random Forrest (rf) obtained the best result among all of the methods with the same accuracy value of 0.889 on all three datasets. Meanwhile, Multinomial Naive Bayes (multnb) achieved the lowest accuracy on the Min-Max based normalized data with an accuracy value of 0.716.

The use of normalization does not make any significant improvement in this case. Only SVM and KNN that have a slight increase in accuracy by using normalization on the dataset. Decision Tree (dt) and Random Forrest (rf) obtained the same result on all three dataset types while Bernoulli Naive Bayes achieved the same accuracy on None Normalised data and normalized data using Min-Max. To be noted, Multinomial Naive Bayes cannot classify normalized data using Z-score because this classifier cannot get negative value as the input. On the None Normalised dataset, there is no feature with a negative value. After normalized using Z-score, there are several negative values so that it does not suitable with the Multinomial Naive Bayes requirement.

Table 7.7: Role Classification Model Accuracy

Method	None Normalised data	Normalized data (Z-score)	Normalized data (Min-Max)
multnb	**0.881**	-	0.715
bernnb	**0.774**	0.733	**0.774**
nn	**0.886**	0.868	0.878
knn	0.858	0.865	**0.888**
lr	**0.882**	0.879	0.852
rf	**0.889**	**0.889**	**0.889**
dt	**0.889**	**0.889**	**0.889**
svm	0.871	**0.875**	0.862

Table 7.8: Anomaly Detection Result using Hard Classification Approach on None Normalised Data

Method	Acc	Prec	Rec	F1
multnb	0.880	0.037	0.698	0.071
bernnb	0.776	0.025	0.868	0.048
nn	0.909	0.045	0.642	0.084
knn	0.873	0.030	0.585	0.057
lr	0.891	0.046	0.792	0.087
rf	0.913	0.041	0.547	0.076
dt	0.913	0.050	0.679	0.093
svm	0.909	0.046	0.660	0.086

Table 7.9: Anomaly Detection Result using Hard Classification Approach on Normalized Data (Z-Score)

Method	Acc	Prec	Rec	F1
multnb	-	-	-	-
bernnb	0.728	0.020	0.868	0.040
nn	0.914	0.049	0.660	0.091
knn	0.893	0.032	0.528	0.060
lr	0.879	0.025	0.472	0.048
rf	0.913	0.041	0.547	0.076
dt	0.914	0.050	0.679	0.093
svm	0.889	0.023	0.396	0.044

Table 7.10: Anomaly Detection Result using Hard Classification Approach on Normalized Data (Min-Max)

Method	Acc	Prec	Rec	F1
multnb	0.715	0.019	0.849	0.037
bernnb	0.776	0.025	0.868	0.048
nn	0.910	0.039	0.547	0.073
knn	0.913	0.041	0.547	0.075
lr	0.847	0.009	0.208	0.017
rf	0.913	0.041	0.547	0.076
dt	0.913	0.050	0.680	0.093
svm	0.857	0.007	0.151	0.014

7.3.2 Anomaly Detection result

The anomaly detection results using Hard Classification approach are displayed in Table 7.8, 7.9, 7.10. In terms of accuracy, generally Random Forrest (rf), Decision Tree (dt), and neural network (nn) have the best result. In terms of precision, Decision Tree (dt) has the best result but it is still very low (0.050). Decision Tree (dt) also has the best result for F1-score. Meanwhile, Naive Bayes methods (multnb and bernnb) have the best result in terms of recall. It can also be seen from the results that the use of normalization does not have any improvement for anomaly detection using the Hard Classification approach.

Overall, using this approach, the anomaly detection methods achieved very good accuracy and adequate recall but low precision and F1-score. Despite all of the machine learning methods used to have good accuracy, we cannot conclude that all of the methods are good to detect an anomaly. It is important to note that the dataset is unbalanced. The number of normal data is far higher than the number of anomaly data. A method could have a good accuracy even though the TP is very low as long as the TN is high. In other words, a method could still have good accuracy even though it cannot detect the anomaly. The good accuracy does not always mean that a method is good enough for detection for this case. In an extreme case, because the number of normal data is far more than the anomaly data, the accuracy would still very good even though a method predicts all of the data as normal. Therefore, accuracy alone is not suitable for the anomaly detection task evaluation in this work and we need to see the other measurements such as precision, recall, and F1. Based on the fact that recall of all of the methods is quite good but the precision is very low, it can be agreed that in all of the methods the number of FP is high but the number of FN is low. It means that there are many normal data that are wrongly classified as an anomaly but there only a few anomaly data that are wrongly classi-

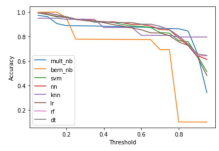
fied as normal. The high recall is actually good if the data that are predicted anomaly will be investigated again so that most of the actual anomaly data will not be missed.

Meanwhile, using the Soft Classification approach, the threshold become a significant factor for the performance like shown in Fig. 7.5, 7.6, 7.7, 7.8 . As expected, generally, the higher threshold, the higher recall, and the lower the precision. It happens because a lower threshold will give more tolerance for the activity to be called normal. The consequences of a low threshold are there are more data classified as normal and fewer data classified as anomaly so that the precision of the method to detect anomaly become higher but the recall becomes lower. Otherwise, a higher threshold provides a high qualification for the data in order to be classified as normal. As the result, there are fewer data classified as normal and more data classified as anomaly so that the precision of the method to detect anomaly becomes lower but the recall becomes higher. Generally, the best result is achieved when the threshold used is 0.1. Table 7.11 shows the F1-score of anomaly detection result using Soft Classification with a threshold value of 0.1. Bernoulli Naive Bayes unexpectedly achieved the best F1-Score on the None Normalised data with a quite high score (0.893). The use of binary features employed by Bernoulli Naive Bayes has become very effective for this task.

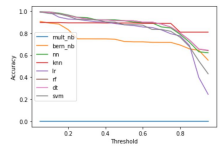
The experiment results also show that generally, the Soft Classification approach obtained better performance than the Hard Classification approach. It happens because the activity of different roles can be very similar so that giving a tolerance can improve the performance. However, apart from Soft Classification based Bernoulli Naive Bayes method, the performance of the proposed method is still low.

Table 7.11: F1-Score of Anomaly Detection Result using Soft Classification Approach with Threshold = 0.1

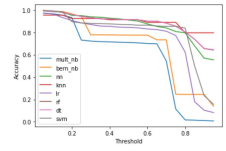
Method	None Normalised data	Normalized data (Z-score)	Normalized data (Min-Max)
multnb	0.152	-	0.243
bernnb	0.893	0.091	0.457
nn	0.208	0.548	0.214
knn	0.375	0.046	0.095
lr	0.115	0.206	0.032
rf	0.264	0.377	0.355
dt	0.383	0.482	0.485
svm	0.507	0.184	0.075



(a) Result on None Normalised Data

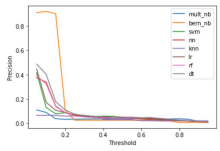


(b) Result on Normalized Data (Z-Score)

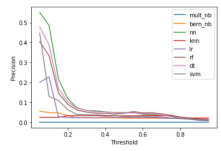


(c) Result on Normalized Data (Min-Max)

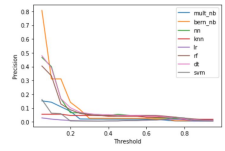
Figure 7.5: Accuracy of Anomaly Detection using Soft Classification



(a) Result on None Normalised Data

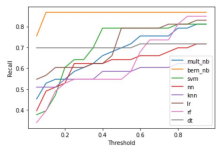


(b) Result on Normalized Data (Z-Score)

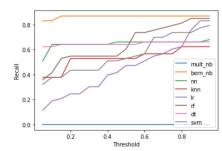


(c) Result on Normalized Data (Min-Max)

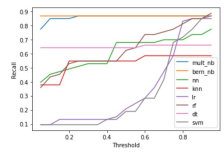
Figure 7.6: Precision of Anomaly Detection using Soft Classification



(a) Result on None Normalised Data

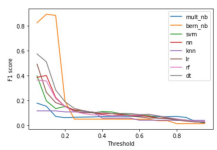


(b) Result on Normalized Data (Z-Score)

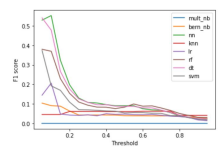


(c) Result on Normalized Data (Min-Max)

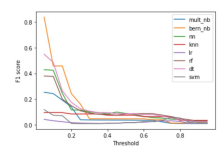
Figure 7.7: Recall of Anomaly Detection using Soft Classification



(a) Result on None Normalised Data



(b) Result on Normalized Data (Z-Score)



(c) Result on Normalized Data (Min-Max)

Figure 7.8: F1-score of Anomaly Detection using Soft Classification

7.4 Discussion

Following the surge in data breaches within healthcare in recent years [7, 12, 32, 30, 27, 5] and their related life-threatening consequences [1], there is the need to analyse healthcare security practices in various ways. One of the ways is the analysis of EHR logs in the context of big data[30, 31, 33]. According to [30] the accesses of healthcare staff can be reconstructed to form their unique profiles. As healthcare personnel frequently access electronic healthcare records for therapeutic and other functions, the logs can be analysed with the suitable machine learning methods to detect anomalies and if possible to determine maliciousness. The healthcare staff's access can be broad in self-authorization or "break the glass" scenarios and this can make it complex for the IT personnel in the hospital to manually determine unauthorised accesses such as insider or outsider masquerades.

To this end, we focused on comparing machine learning classification methods using simulated logs of EHR. The simulated data of EHR logs in this study was quite useful since the different types of machine learning algorithms needed to be evaluated to assess the performance of the methods [17] prior to usage in real applications. Health record logs data is confidential and most hospitals do not want to take the risk in sharing their logs. Clearly, real EHR logs or semi-synthetic data could be the better option in the assessment. However, EHR logs is very sensitive and there are regulatory hurdles and stringent privacy laws across the globe[29] that are protecting the sensitive healthcare data. So hospitals are not willing to risk in giving out such data. To succeed in accessing the performance of the machine learning algorithms amidst these challenges, a simulated synthetic data was a clear choice to serve as a playground or a test range for comparing the suitability of these algorithms for analysing healthcare security practice without violating security and privacy laws [4]. Yeng et al adopted similar approach in testing algorithms towards detecting disease outbreak [29]. Therefore, simulated electronic health record logs data was used in this work.

We used a role classification based anomaly detection method because users with the same roles tend to have similar activity while users with different roles tend to have different activities[3, 34, 6, 20]. The experiment results show that all of the machine learning method employed shows a good accuracy for roles classification as shown in figure 5. However, despite the good accuracy and recall, the methods still have a low performance in detecting anomaly in terms of precision and F1-score as shown in figure 6, figure 7 and figure 8. The high recall is actually good for the data administrators if they undergo further investigation. That way, most of the actual anomaly data will not be missed. Usually, in the hospital, broad access is given to healthcare staff through self-authorisation but this require the the IT staffs to manually evaluate the anomaly and malicious access [24]. There-

fore, the result from this work can be used by the hospital to narrow down the data for the manual investigation work.

The experiment results also show that generally, the Soft Classification approach achieved better performance than the Hard Classification approach as shwon in figure 7. It happens because the activity of different roles can be very similar so that giving a tolerance can improve the performance. The use of normalization also did not give any improvement to the performance. The best performance is obtained using Bernoulli Naive Bayes on the None Normalised data with an F1-score of 0.893.

7.5 Conclusion

Due to the recent increases in data breaches within healthcare, we compared various machine learning classification methods using simulated EHR logs towards determining anomalies. The experiment results show that all of the methods used achieved quite a good accuracy for role classification. For the anomaly detection, generally, all of the methods obtained a high recall and accuracy but low precision and F1-score. This high recall means that the method from this work can be a good tool to narrow down the data for further manual investigation. Since the activity of different role can be very similar, Soft Classification approach performed better than the Hard Classification approach because the former provides some tolerances. The best performance is obtained using Bernoulli Naive Bayes on the None Normalised data with an F1-score of 0.893.

In fact since anomaly detection does not entirely means maliciousness, future works on further processing the anomalies to detect malicious activities. Besides, since real EHR logs data have not been used for such a comparison, the use of real data instead of simulated one can give a better insight. Additional, as labeled real data are hard to get, it is also important to compare unsupervised methods for the detection of anomalies and maliciousness in the context big data.

7.6 Bibliography

[1] ASSOCIATEDPRESS. German hospital hacked, patient taken to another city dies. Available from: "`https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies`". 198, 217, 224

[2] BODDY, A., HURST, W., MACKAY, M., AND EL RHALIBI, A. A study into detecting anomalous behaviours within healthcare infrastructures. In *2016 9th International Conference on Developments in eSystems Engineering (DeSE)* (2016), IEEE, pp. 111–117. 12, 15, 200, 227, 228

[3] BODDY, A. J., HURST, W., MACKAY, M., AND EL RHALIBI, A. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 13, 15, 147, 148, 200, 201, 217, 227, 228

[4] BURGARD, J. P., KOLB, J.-P., MERKLE, H., AND MÜNNICH, R. Synthetic data for open and reproducible methodological research in social sciences and official statistics. *AStA Wirtschafts-und Sozialstatistisches Archiv 11*, 3-4 (2017), 233–244. 217

[5] CANNOY, S. D., AND SALAM, A. A framework for health care information assurance policy and compliance. *Communications of the ACM 53*, 3 (2010), 126–131. 12, 199, 200, 217

[6] CHEN, Y., NYEMBA, S., ZHANG, W., AND MALIN, B. Specializing network analysis to detect anomalous insider actions. *Security informatics 1*, 1 (2012), 1–24. 13, 15, 200, 202, 217

[7] EHRENFELD, J. cybersecurity and health information technology: A time to act, 2017. 199, 217

[8] FERNANDEZ-ALEMAN, J. L., SANCHEZ-HENAREJOS, A., TOVAL, A., SANCHEZ-GARCIA, A. B., HERNANDEZ-HERNANDEZ, I., AND FERNANDEZ-LUQUE, L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics 84*, 6 (2015), 454–467. 12, 15, 200, 406, 414, 415

[9] GORDON, W. J., WRIGHT, A., AIYAGARI, R., CORBO, L., GLYNN, R. J., KADAKIA, J., KUFAHL, J., MAZZONE, C., NOGA, J., PARKULO, M., ET AL. Assessment of employee susceptibility to phishing attacks at us health care institutions. *JAMA network open 2*, 3 (2019), e190393–e190393. 11, 14, 15, 200, 272, 280, 284, 285, 297, 298, 492

[10] GORDON, W. J., WRIGHT, A., GLYNN, R. J., KADAKIA, J., MAZZONE, C., LEINBACH, E., AND LANDMAN, A. Evaluation of a mandatory phishing training program for high-risk employees at a us healthcare system. *Journal of the American Medical Informatics Association 26*, 6 (2019), 547–552. 14, 15, 200, 272, 284, 285, 297, 491, 492

[11] GUPTA, S., HANSON, C., GUNTER, C. A., FRANK, M., LIEBOVITZ, D., AND MALIN, B. Modeling and detecting anomalous topic access. In *2013 IEEE International Conference on Intelligence and Security Informatics* (2013), IEEE, pp. 100–105. 201

[12] HEALTHITSECURITY. Incentivize cybersecurity best practices for data security, 2017. Available from: `https://healthitsecurity.com/news/incentivize-cybersecurity-best-practices-for-data-security`. 199, 217

[13] HIMSS. So you've been hit with a ransomware attack. what now? Available from: "https://www.healthcareitnews.com/news/so-youve-been-hit-ransomware-attack-what-now". 199

[14] HOFMANN, T., PUZICHA, J., AND JORDAN, M. I. Learning from dyadic data. In *Advances in neural information processing systems* (1999), pp. 466–472. 201

[15] HUMAIDI, N., AND BALAKRISHNAN, V. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR* (2012), vol. 35, IACSIT Press Singapore, pp. 1–6. 12, 15, 200, 272, 274

[16] ISO. 27799:2016(en), health informatics information security management in health using iso/iec 27002. 2016., November 2016. 2, 6, 198

[17] JAFARPOUR KHAMENEH, N. *Machine Learning for Disease Outbreak Detection Using Probabilistic Models*. Ph.D. thesis, École Polytechnique de Montréal, 2014. 217

[18] KONONENKO, I., AND KUKAR, M. *Machine learning and data mining*. Horwood Publishing, 2007. 202

[19] LI, X., XUE, Y., AND MALIN, B. Detecting anomalous user behaviors in workflow-driven web applications. In *2012 IEEE 31st Symposium on Reliable Distributed Systems* (2012), IEEE, pp. 1–10. 148, 202

[20] MENON, A. K., CHITRAPURA, K.-P., GARG, S., AGARWAL, D., AND KOTA, N. Response prediction using collaborative filtering with hierarchies and side-information. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining* (2011), pp. 141–149. 201, 217

[21] MENON, A. K., JIANG, X., KIM, J., VAIDYA, J., AND OHNO-MACHADO, L. Detecting inappropriate access to electronic health records using collaborative filtering. *Machine learning 95*, 1 (2014), 87–101. 201

[22] RADHAKRISHNA, R. B. Tips for developing and testing questionnaires/instruments. *Journal of extension 45*, 1 (2007), 1–4. 200

[23] ROSCH, E. H. On the internal structure of perceptual and semantic categories. In *Cognitive development and acquisition of language*. Elsevier, 1973, pp. 111–144. 200

[24] RØSTAD, L., AND EDSBERG, O. A study of access control requirements for healthcare systems based on audit trails from access logs. In *22nd Annual Computer Security Applications Conference (ACSAC 2006), 11-15 December 2006, Miami Beach, Florida, USA* (2006), IEEE Computer Society, pp. 175–186. 152, 201, 202, 217, 225, 226, 247

[25] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 9, 10, 12, 15, 200, 274, 405, 407, 412, 428, 446, 457

[26] SEARCHHEALTHIT. Hospital takes aim at patient health data security with ai tools, 2019. Available from: `hhttps://searchhealthit.techtarget.com/feature/Hospital-takes-aim-at-patient-health-data-security-with-AI-tools`. 199

[27] VERISON. Data breaches report. 2019, 2019. Available from: `https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf`. 199, 217, 224

[28] WRIGHT, A., AARON, S., AND BATES, D. W. The big phish: cyberattacks against us healthcare systems, 2016. 14, 15, 200

[29] YENG, P., WOLDAREGAY, A. Z., AND HARTVIGSEN, G. K-cusum: Cluster detection mechanism in edmon. 25, 217, 234, 249, 298

[30] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[31] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 11, 15, 22, 138, 200, 217, 224, 236, 273, 274, 404, 406, 407, 409, 414, 426, 442, 491, 498

[32] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 1, 2, 6, 10, 11, 15, 17, 23, 199, 217, 224, 274, 282, 404, 405, 406, 407, 409, 410, 414, 442, 443, 454, 457, 491, 498

[33] YENG, PROSPER KANDABONGEE AND NWEKE, LIVINUS OBIORA AND WOLDAREGAY, ASHENAFI ZEBENE AND YANG, BIAN AND

SNEKKENES, EINAR ARTHUR. Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. In *Proceedings of SAI Intelligent Systems Conference* (2020), Springer, pp. 1–18. 11, 19, 23, 200, 201, 202, 217, 247

[34] ZIEMNIAK, T. Use of machine learning classification techniques to detect atypical behavior in medical applications. In *2011 Sixth International Conference on IT Security Incident Management and IT Forensics* (2011), IEEE, pp. 149–162. 200, 201, 217, 227

2020 International Conference on Computational Science and Computational Intelligence (CSCI)
https: //doi.org/10.1109/CSCI51800.2020.00143

Chapter 8

Workflow-based anomaly detection using machine learning on electronic health records' logs: A Comparative Study.

2020 International Conference on Computational Science and Computational Intelligence (CSCI)

Prosper K. Yeng, Muhammad A. Fauzi, and Bian Yang

Abstract

Timely access to patients' healthcare records is very essential. As a result, broad access to EHR is mostly provided to users in effort towards complying with the availability trait of the CIA. However, this opens up the system for abuse and misuse. This paper, therefore, analyzed the workflows of healthcare staff's security practices in electronic health records (EHR) logs to determine anomalous security practices. Different classification types of machine learning algorithms were used. The EHR logs were simulated based on healthcare workflow scenarios. A number of machine learning algorithms were used to analyze the logs for deviations of accesses from the workflow. Based on the analysis results, all of the machine learning methods generally obtained a very good performance. The best performance on the non-normalized dataset is achieved by the Logistic Regression method with accuracy, precision, recall, and F1 value of 0.998, 0.849, 0.978, and0.909 respectively while Random Forest obtained the best result on Normalized data with accuracy, precision, recall, and F1 value of 0.998, 0.867, 0.836, and 0.851 respectively. It however remains challenging to detect malicious security practice if a malicious actor follows the workflow to access healthcare records with legitimate access right.

8.1 Introduction

The adverse impacts in data breaches within healthcare are no longer hypothetical statements but realities that are causing harm to innocent data sub-

jects, healthcare providers, and other stakeholders. For instance, in Finland, there was a data breach in 2018 and 2019 on Vastaamo, a center for psychotherapy which has 20 clinics located in different places [10]. The breach resulted in compromising about 300 patients records of which several of the affected data subjects have been demanded by the hackers to pay a ransom of about 500 Euros each in bitcoin or else, their data will be released to the public. In a related incident in September 2020, there was a ransomware attack at Duesseldorf University Clinic in Germany. As a result, the medical records of a patient were not timely available during an emergency and this resulted in the death of that patient [1].

Though the cause of these breaches was not disclosed, most of the data breaches in recent times have been attributed to human factors[18, 19] through the usage of social engineering tricks and other techniques [9, 4]. Technological countermeasures (eg firewalls, intrusion detection and prevention systems, antivirus, etc) have been the default and traditional methods[23]. These countermeasures have therefore been strengthened, making it more difficult for the circumvention of hackers. So, the hackers tend to exploit the human elements who are the weakest link in the security chain[13, 16, 22]. Some legitimate users with access rights can also tend to sell their access credentials to hackers thus complicating the security measures. The data breaches continue to increase in healthcare based on human factors According to the IBM report, the healthcare sector has recorded the costliest data breaches among various sectors in the aspect of the cost of loss of business, ex-post response, notification, and detection, and escalation[11].

To this end, various efforts are being adopted to minimize the data breaches in healthcare which includes a comprehensive approach involving modeling and analyzing healthcare security practice in the context of big data [22].

The general objective of this paper is to therefore analyze simulated electronic healthcare records logs with the aim to compare various classification methods. The most effective and efficient algorithms are to be adopted towards analyzing real EHR logs to determine anomalies towards developing security countermeasures.

8.1.1 Security requirement in EHR

Security measures in EHR need to conform with the confidentiality, integrity, and availability (CIA) traits requirements. For instance, in complying with the Norwegian code of conduct for healthcare security practices[8, 21]:

- Patients records need to be accessed for therapeutic purposes
- Access must be granted following a specific decision based on the completed or planned implementation of measures for the medical treatment of the patient. So access must be provided to comply with

the confidentiality rules. This means access to personal health data and personal data is given to only those with an official need to use.

- In the case of data exchange between organizations, the hospital needs to have the technical and organizational solutions to prevent access to health data as specified within the CIA traits, including authorized access with adequate authentication and least privileges.
- In self-authorization or "break the glass" scenarios, the necessary measures should be provided to enable access to patient information when necessary. However, misuse of self-authorization needs to be handled as a breach[8, 21, 15].
- EHR with permission functions must record rights to read, register, correct, erase, and/or block personal health data and personal data in the access management.

The logs must contain the following[8, 21, 15]:

- unique identifier for the authorized user
- The role of the authorized user at the time of access
- Organisational affiliation
- Organisational affiliation of the authorized person
- Type of data to which access has been gained
- The user who disclosed health data that is linked to the name or national ID number of the patient or health care user
- Basis for the access
- Time and duration of access.

Additionally, Confidentiality measures need to include the following[21]:

- Persons outside the organization must not gain unauthorized access to EHRs
- Persons within the organization must be given access in accordance with established principles for access control especially based on the need to use basis.
- Details of persons who gained access (entered records, changes, corrections, and deletions) need to be registered in the logs to ensure audit trail to the origin.

- Persons or technologies, within or outside the organization, must not be able to access healthcare data without appropriate authorization.
- Personal health data and personal data must be linked to an identifiable person and must be accurate.

In the context of availability, personal health data and personal data must be accessible when there is an official need to access such data amidst the confidentiality framework. Self-authorization or "break the glass" may be established to provide access to authorized users to access EHR without following the conventional authorization procedures on the basis of the need to use. But established procedures need to be established, the reason for and self-authorization must be documented. All misuse of self-authorization must be followed up as a breach.

8.1.2 Problem statement, scope and contribution

In this work, we hypothesized that anomaly behavior can be detected effectively if we model and analyze the normal healthcare staff behavior of a hospital in general. This can be achieved by considering all other activities that deviate from the normal workflow (as specified in section 8.1.1) as an anomaly. An establishment of normal behavior at the hospital level, in general, is considered in this work, having consolidated all activities to establish the normal behavior pattern. For this purpose, we developed a health information system workflow to simulate health records logs data. The simulation is based on the general workflow in the hospital. This data is then used for the anomaly detection task. We extract several features from this data for the anomaly detection task. Furthermore, a comparative analysis is conducted by applying several machine learning classifiers to do the detection. The feature selection and normalization scenarios are also performed in this work.

8.1.3 Related work

Timely access to patients healthcare records is mostly essential. As a result, broad access to EHR is mostly provided to users in efforts towards complying with the availability trait of the CIA[15]. However, this opens up the system for abuse and misuse[15]. Based on that, Zhang et al., hypothesized and model the patient care pathways as a progression of a patient through the healthcare system [24]. So the patient flow was modeled as a sequence of accesses of the users defined in the form of a graph and further modeled the trend of patients records accesses which showed deviations from patients care pathways. Graph-based approach was used to model the accesses of patients records in EHR in the context of patient care. A three-month EHR logs was used to evaluate the framework. The framework detected some

outliers and deviations of accesses which were different from various types of medical accesses. There was also a high deviation of normal access patterns of nonclinical healthcare workers from clinical users. The ROC curve for the prediction showed 92%, suggesting the performance of the approach was efficient. Additionally, Ziemniak et al used C4.5 decision tree to detect abnormal security behaviour in a healthcare application. Ad-hoc analyis was used to determine atypical behaviour by visually looking for interesting nodes such as path-length investigation [25]. These studies ,[24, 25], adopted the general work-flow in accessing patients records which yielded a good results but each of them only adopted to graph-based approach in their work without comparing other methods (such as Nearest neighbor, Bayesian probability methods, support vector machine (SVM) etc) to exhibit their performance measure. Due to the nature of data (eg noisy or not noisy), the performance of algorithms differ. Therefore, in effort to analyse security practice in EHR logs, it is important to compare the performance of algorithms to select the most efficient and effective method for the purpose.

In a related work, Boddy et al tried to avert challenges in restrictions of access controls, often faced by both patients and healthcare workers in EHRs. So human-in-the-loop model was developed by Boddy et al using logs of EHR[2].The model was assessed for anomaly using the human-in-the-loop model with local outlier factor (LOF). A weighted average was applied to each audit log and their respective anomaly scores were computed. The computed average score of the ensemble were plotted against the date and time stamp. The output was visualized for the analysis. The model was able to detect 145 anomalous activities using unlabelled dataset.Additionally, Boddy et al adopted density-based local outlier detection model to profile users' behaviour in relation to their security practice[3]. A local outlier detection factor (LOF) assesses the local deviations from similar group of users (eg doctors, nurses etc) by measuring the isolated distance of a data point to its k-nearest neighbours.

Additionally, Chen et al., developed a framework for anomalous insiders from access logs called community-based anomaly detection system [5]. The detection is based on the behaviour of users and their relation with each other. The model is based on the hypothesis that typical users mostly form and function as communities. So the access logs of users were mined and modeled for the relation of users and their behavioural profiles. Based on the accesses of users, a typical user's accesses of objects should be similar to the peers. For instance, in EHR, a typical user such as a nurse should access similar set of patients records like other nurses due to commonalities in patient care path-ways. Principal Component Analysis (PCA) was relied on to develop an intrusion detection model. The PCA was applied on training features to determine the major and minor principal components for the model. k-Nearest neighbor was was found for each user and calculated the

deviation of each of the users from their nearest neighbours. The experimental result showed that, the CAD was able to distinguish anomalous users in a real data log.

While the studies by [2, 3, 5] showed good performances, a comparative analysis was not also considered. To this end we analyzed simulated EHR logs to compare neural network (nn), LogisticRegression (lr), Random Forrest (rf), decision tree (dt), Support Vector Machine (svm), K-nearest neighbor (knn), Naive Bayes multi-nomial (mulnb) and Naive Bayes binomial(bennb) methods by analysing for deviations from the workflows.

8.2 Our Method

8.2.1 Health record logs data simulation

We developed a hospital information system work-flows to simulate healthcare record log data for this work. This system has five main modules including Patient Management, Pharmacy Management, Laboratory Management, Finance, and Reporting. In this simulation, the hospital is assumed to have 19 departments including IT, Finance, Administration, Laboratory, Pharmacy, Emergency, 10 Out Patients departments (Ear-Nose-Throat, Eyes, Tooth, Child, Orthopedic, Neurological, Gynecological, Diabetes, Rheumatology, and Cancer), with 3 In Patients Departments. Meanwhile, the professions employed by the hospital in this simulation include Head of IT (HIT), Technical Support (TS), Head of Finance (HF), Finance Staff (FS), Head of Administration (HA), Staff of Administration (SA), Head of Lab (HL), Lab Assistant, (LA), Head of Pharmacy (HP), Pharmacy Assistant (PA), Doctor (DO), and Nurse (NU).

Two types of shifts are applied in this simulation: the daily shift and the three 8-hour shift. The daily shift is from 08.00-16.00 Monday to Friday, while three 8-hour shifts involve three shifts each day: a) Shift 1: 06.00-14.00, b) Shift 2: 14.00-22.00, and c) Shift 3: 22.00-06.00 (next day). The details of the shift and schedule including the number of staffs and professions in each shift are displayed in Table 8.1 and 8.2.

The inpatient, outpatient, and emergency department patient flow is shown in Fig. 8.1, 8.2, and 8.3, respectively. Under the described simulation setting and this patient flow, a one-year health record log data are simulated starting from 1 January 2019 until 31 December 2019. The logs are considered as normal data (non-anomaly). In addition, we also generate some abnormal data by simulating attackers who are assumed to have stolen the passwords of certain users and use it to access records of patients (e.g. identity theft). The attackers are simulated to frequently do not follow the hospital flows and tend to deviate from expected behaviors (e.g. make more transactions than the actual users) [14]. In our simulation system, 21

Table 8.1: Daily Shift

Shift ID	Department	Profession (number of staffs)
0	IT	HIT(1), TS(2)
1	Finance	HF(1), FS(4)
2	Administration	HA(1), SA(2)
3	Laboratory	HL(1), LA(5)
4	Pharmacy	HP(1), PA(2)
5	Out Patients Ear-Nose-Throat	DO(1), NU(2)
6	Out Patients Eyes	DO(1), NU(2)
7	Out Patients Tooth	DO(1), NU(2)
8	Out Patients Child	DO(1), NU(2)
9	Out Patients Orthopedic	DO(1), NU(2)
10	Out Patients Neurological	DO(1), NU(2)
11	Out Patients Gynecological	DO(1), NU(2)
12	Out Patients Diabetes	DO(1), NU(2)
13	Out Patients Rheumatology	DO(1), NU(2)
14	Out Patients Cancer	DO(1), NU(2)
16	In Patients Ward1	DO(1)
17	In Patients Ward2	DO(1)
18	In Patients Ward3	DO(1)

fields are recorded as depicted in Table 8.3. As the result, 283,678 logs were produced with 274,983 of them are legitimate access while 8,695 of them are anomalous accesses.

Table 8.2: Three 8-hour shift

Shift ID	Department	Profession (number of staffs)
15	Emergency	DO(2), NU(7)
16	In Patients Ward1	NU(2)
17	In Patients Ward2	NU(2)
18	In Patients Ward3	NU(2)

8.2.2 Proposed method for anomaly detection

The anomaly detection used in this work is using a data-driven method by applying machine learning classifiers. Data-driven is a popular approach in anomaly detection and proven to get promising performance [6, 12]. The classifier learns from the labeled dataset to determine normal and abnormal

Table 8.3: Record Fields

Number	Field Name	Description
1	start_access_time	The starting time the staff accesses the patient record.
2	end_access_time	The end time the staff accesses the patient record access.
3	staff_ID	The ID of the staffs who do the activity
4	role_ID	The role of the staff who access the patient record
5	patient_ID	The ID of the patient whose record is being accessed
6	activity_ID	The ID of the activity (1: Create, 2: Read, 3:Update, 4: Delete)
7	staff_department_ID	The department of the staff who do activity
8	staff_organization_ID	The organization of the staff who access the patient record
9	device_ID	The ID of the computer used by the staff to access patient record
10	browser_ID	The browser used by the staff to access patient record
11	ip_address	The IP Address of the computer used by the staff to access patient record
12	reason_ID	The reason of staff access the patient record (optional)
13	shift_ID	The ID of shift the staff belong to on the day of patient access record
14	sift_start_time	The start time of shift the staff belong to on the day of patient access record
15	sift_end_time	The end time of shift the staff belong to on the day of patient access record
16	module	The module acessed by the staff

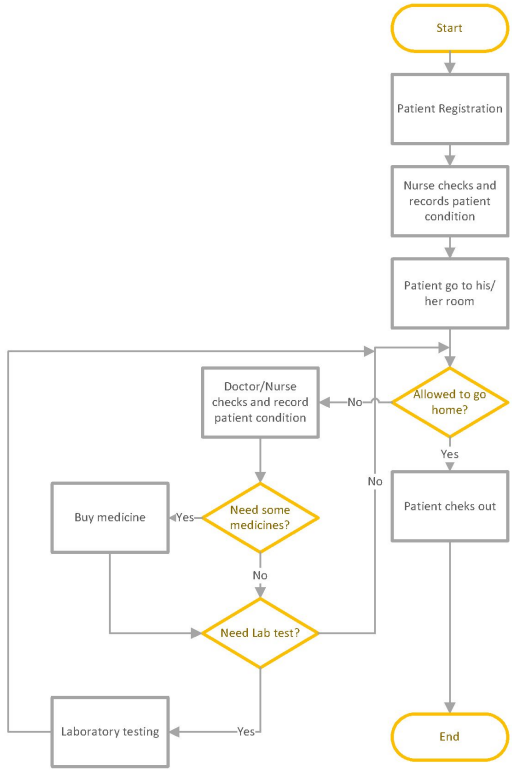


Figure 8.1: The Inpatients Department Flow

activities. This model is then used to detect deviations or anomaly from normal behavior.

8.2.2.1 Data Preparation

Each log record in the dataset portrays a single activity of a user. In order to get a good understanding of the user's behavior, we need to combine several activities from a particular period. Hence, in this work, the raw log data were processed into 24-hour blocks such that an instance reflects a user's cumulative activity in a single day. 24,648 instances were extracted from the raw logs as the outcome with 24,286 of them are labeled as normal data and 362 of them are labeled as anomaly data. The instances are labeled as an anomaly when they had at least one abnormal log access in a single day while the labeled normal instances are all the instances whose all logs are legitimate access.

8.2.2.2 Feature Extraction

After the log combination process, several features are extracted from each instance. The list of features used in this work is displayed in Table 9.6. In addition, we also applied the Min-Max normalization method and Chi-Square based feature selection to the feature data.

8.2.2.3 Anomaly Detection

After the features are extracted, we use 9 machine learning methods including Multinomial Naive Bayes (multnb), Bernoulli Naive Bayes (bernnb), Gaussian Naive Bayes (gaussnb), Support Vector Machine (svm), Neural Network (nn), K-Nearest Neighbours (knn), Logistic Regression (lr), Random Forest (rf), and Decision Tree (dt). To evaluate the methods, the data is divided into training and testing. Logs from January until August are employed as training data while logs from September until December are utilized as testing data. Using the extracted features and the training data, each machine learning classifier is trained. Furthermore, this trained classifier is employed to do the anomaly detection task. Accuracy, precision, recall, and f1-measure are the metric used for evaluation.

8.2.3 Performance Evaluation

Several assessments were employed to evaluate the result including Accuracy (Acc), Precision (Prec), Recall (Rec), and F_1-score (F_1). We calculated all of the evaluation measures based on the confusion matrix shown in Fig. 8.4. True Positive (TP) and True Negative (TN) are the numbers of data that were correctly classified. TP is the number of anomaly data correctly classified into the anomaly category, while TN is the number of normal data correctly classified into the normal category. Meanwhile, False Positive (FP), or also referred to as Type I Error, is the number of data that actually belongs to the normal category but incorrectly classified into the anomaly category. On the other hand, False Negative (FN) or Type II Error is the number of anomaly data incorrectly classified as normal data. The formulas for the measurement are as follows:

$$Acc = \frac{TP + TN}{TP + FP + FN + TN} \tag{8.1}$$

$$Prec = \frac{TP}{TP + FP} \tag{8.2}$$

$$Rec = \frac{TP}{TP + FN} \tag{8.3}$$

$$F_1 = 2\frac{P \cdot R}{P + R} \tag{8.4}$$

Table 8.4: Dataset Feature Name and Description

Feature Name	Description
create_activity	Number of 'create' transactions conducted in a single day
rea_activity	Number of 'read' transactions conducted in a single day
update_activity	Number of 'update' transactions conducted in a single day
delete_activity	Number of 'delete' transactions conducted in a single day
all_patient_record	Number of access to the patient records in a single day
unique_patient	Number of unique patients whose records has been accessed in a single day
modules	Number of kind of modules in the information system accessed in a single day
report_module_access	Number of transactions conducted in the report module in a single day
finance_module_access	Number of transactions conducted in the finance module in a single day
patient_module_access	Number of transactions conducted in the patient management module in a single day
lab_module_access	Number of transactions conducted in the laboratory module in a single day
pharmacy_module_access	Number of transactions conducted in the pharmacy module in a single day
outside_access	Number of transactions conducted from outside hospital network in a single day
browsers	Number of browser type used in a single day
number of chrome	Number of chrome browser used in a single day
ie_access	Number of Internet Explorer browser used in a single day
safari_access	Number of Safari browser used in a single day
firefox_access	Number of Firefox browser used in a single day
otherbrowser_access	Number of other browser used in a single day

8.3 Experiment Results and Discussion

Due to the sensitive nature of healthcare records, it is sometimes challenging for hospitals to overcome the legal and regulatory hurdles in order to provide such logs for experimental purposes. Meanwhile, the importance to assess algorithms to select the most effective and efficient ones for real implementation can not be downplayed. So the better option is to simulate such related data logs for the data analysis[20]. Therefore, we simulated EHR logs to analyze the security practices of healthcare professionals.

Table 8.5: Anomaly Detection Result on Non-normalized Data

Method	Acc	Prec	Rec	F1
multnb	0.955	0.735	0.101	0.178
bernnb	0.997	**0.867**	0.754	0.807
gaussnb	0.995	**0.867**	0.613	0.718
knn	0.997	0.698	0.840	0.762
nn	**0.998**	0.830	0.880	0.854
lr	**0.998**	0.849	**0.978**	**0.909**
rf	**0.998**	**0.867**	0.836	0.851
dt	0.997	**0.867**	0.807	0.836
svm	**0.998**	0.811	0.977	0.886

Table 8.6: Anomaly Detection Result on Min-Max based Normalized Data

Method	Acc	Prec	Rec	F1
multnb	0.995	0.358	**1.000**	0.527
bernnb	0.997	**0.867**	0.779	0.821
gaussnb	0.995	**0.867**	0.621	0.724
knn	0.997	0.698	0.948	0.804
nn	0.996	0.490	0.928	0.641
lr	0.996	0.433	**1.000**	0.605
rf	**0.998**	**0.867**	0.836	**0.851**
dt	0.997	**0.867**	0.793	0.828
svm	0.996	0.433	0.958	0.597

The anomaly detection results on the non-normalized data are displayed in Table 8.5. In terms of accuracy, generally, Neural Network, Logistic Regression, Random Forrest, and Support Vector Machine have the best result with 0.998. However, the accuracy value difference between the best performing methods and the other methods is very insignificant with Multinomial Naive Bayes and Gaussian Naive Bayes as the worst methods still have

an accuracy value of 0.955. In terms of precision, generally, Bernoulli Naive Bayes, Gaussian Naive Bayes, Random Forrest, and Decision Tree have the best result with 0.867. KNN has the lowest precision value with 0.698 and it is quite far below the other methods. Meanwhile, Logistic Regression obtained the best recall and F1 values with 0.978 and 0.909 respectively. Multinomial Naive Bayes, on the other hand, achieved the worst recall and F1 values with 0.101 and 0.178 respectively.

Concerning the accuracy performance, it is important to note that the dataset is unbalanced. Since anomaly data is very rare, most of the dataset for anomaly detection is unbalanced with normal data far more than the anomaly data (e.g. [17, 17]). In this case, it is not effective enough to determine the performance of the methods based on accuracy alone. In the anomaly detection task, since we want to detect an anomaly, we consider the anomaly data as positive data and normal data as negative data. Since the number of negative data is far higher than positive data, the number of TN, in this case, tends to be very high as well. A method with a low TP could still have very good accuracy because the TN is very high. In other words, even if it can not detect the anomaly, a method may still have good accuracy. Even in an extreme case, when the data is highly unbalanced, the accuracy of a method would still very good even though the method predicts all of the data as normal. Hence, accuracy alone is not suitable for the anomaly detection task evaluation if the dataset is unbalanced. Other evaluation methods such as precision, recall, and F1 are needed.

One of the examples of the previously described case can be seen in Table 8.5 where Multinomial Naive Bayes has very good accuracy but a very low F1-score. This method only classifies very little data as anomaly so that the recall is very low. Almost all of the data, including a lot of anomaly data, are classified into normal category. As the consequence, the F1-score becomes very low as well. This method cannot be considered good because it misses a lot of anomaly data and considers them as normal. It could be dangerous because there would be many attacker's actions that would be considered normal if we use this method.

Overall, almost all of the machine learning methods employed for non-normalized data in this work achieved good results except Multinomial Naive Bayes. The explanation about this case can be seen in Fig. 8.5a. There are many irrelevant or noisy features in the dataset. We can see from the figure that almost all of the methods have a very good F1-score even though only use a few features. It means that only some features that can distinguish the anomaly data from normal data well. Some other features are irrelevant or noisy because it can separate the two categories well. In some cases, the noisy features can decrease the performance. Multinomial Naive Bayes suffer a lot from the noisy features. The noisy features give a big influence on this method so that the performance decrease significantly.

The use of normalization in this work generally cannot increase the performance. In fact, it decreases the performance of some methods such as Neural Network, Logistic Regression, and SVM. The explanation about this case can be found in Fig. 8.5b. As described before, there are some noisy features in the dataset and some features are more determinant than others. The important features such as outside_access have a high difference value between that in normal and anomaly data. Normalizing the feature value makes all features appear on similar scales and are all treated as equally important. This condition can decrease the model performance. Therefore, as displayed in Fig. 8.5b, the result of normalized data is generally equal to the result of non-normalized data. After 6 or more features, the performance on the normalized data starts to decline because the method starts to deal with noisy data.

The use of feature selection is proven to give an improvement in the anomaly detection task in this work because of the existence of some noisy data. Chi-square is able to select the best feature used to detect an anomaly. The use of Chi-square based feature selection can improve the performance of all machine learning methods employed by removing several noisy features. Based on the results in Fig. 8.5, the optimal number of features is between 3-6. The other benefit of the use of feature selection is reducing the time complexity to make the method perform faster [7].

8.4 Conclusion and future work

Due to the surge in data breaches within healthcare, there is the need to determine the causes in various ways including big data context[22]. This is because users often leave their traces of accesses in access logs which when analyzed can provide knowledge of access deviations from workflows[21]. To this end, this paper analyzed the workflows of healthcare staff's security practices in simulated electronic health records (EHR) logs to determine anomalous security practices with different classification types of machine learning algorithms. The EHR logs were simulated based on healthcare workflow scenarios. A number of machine learning algorithms were used to analyze the logs for deviations of accesses from the workflow, which is termed as anomaly accesses. The algorithms used were then compared in terms of their performance including accuracy (Acc), precision (Prec), recall (Rec), and F-Measure (F1).

Overall, based on the experiment results, generally, all of the machine learning methods employed in this work perform very well to detect an anomaly. The best performance on the non-normalized dataset is achieved by the Logistic Regression method with accuracy, precision, recall, and F1 value of 0.998, 0.849, 0.978, and 0.909 respectively. Meanwhile, on Normalized data, Random Forest obtained the best result with accuracy, precision,

recall, and F1 value of 0.998, 0.867, 0.836, and 0.851 respectively. However, The use of normalization generally could not increase the performance of the used methods. The results also reveal that there are several noisy features that can affect performance. Therefore, the use of Chi-square as feature selection is very important in this work. This method can select the best feature and remove the bad features so that the performance can be improved. Based on the experiment results, the optimal number of features is between 3-6. The additional advantage of reducing several features is we can also reduce the time complexity to make the method run faster. Therefore, it can be concluded that the proposed workflow based approach can be adopted with the well-performed algorithms for analyzing security practice in real logs of EHR.

It however remains challenging to detect malicious security practice if a malicious actor follows the workflow to access healthcare records with legitimate access rights. Additionally, future works need to further assess the detected anomalies for maliciousness. This will provide more knowledge for the appropriate security measures to be taken. Another aspect that needs to be considered in future works includes assessing the logs with unsupervised methods to compare their performance to be used in scenarios where the EHR logs are unlabeled.

8.5 Bibliography

[1] ASSOCIATEDPRESS. German hospital hacked, patient taken to another city dies. Available from: "https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies". 198, 217, 224

[2] BODDY, A., HURST, W., MACKAY, M., AND EL RHALIBI, A. A study into detecting anomalous behaviours within healthcare infrastructures. In *2016 9th International Conference on Developments in eSystems Engineering (DeSE)* (2016), IEEE, pp. 111–117. 12, 15, 200, 227, 228

[3] BODDY, A. J., HURST, W., MACKAY, M., AND EL RHALIBI, A. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 13, 15, 147, 148, 200, 201, 217, 227, 228

[4] BUTAVICIUS, M., PARSONS, K., PATTINSON, M., AND MCCORMAC, A. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887* (2016). 224

[5] CHEN, Y., AND MALIN, B. Detection of anomalous insiders in collaborative environments via relational analysis of access logs. In *Proceed-*

ings of the first ACM conference on Data and application security and privacy (2011), pp. 63–74. 227, 228

[6] DU, M., LI, F., ZHENG, G., AND SRIKUMAR, V. Deeplog: Anomaly detection and diagnosis from system logs through deep learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (2017), pp. 1285–1298. 229

[7] FAUZI, M. A., ARIFIN, A. Z., GOSARIA, S. C., AND PRABOWO, I. S. Indonesian news classification using naïve bayes and two-phase feature selection model. *Indonesian Journal of Electrical Engineering and Computer Science* 2, 3 (2016), 401–408. 236

[8] FOR E HEALTH, D. Code of conduct for information security and data protection in the healthcare and care services sector, 2018. Available from: `https://ehelse.no/normen/documents-in-english`. 224, 225

[9] HIMSS. Health share of oregon: 654,000 patients. Available from: "`https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far`". 224

[10] HJELLEN, B. Hacking scandal shakes finland - patients pressured for money. Available from: "`https://www.nrk.no/urix/hacking-skandale-ryster-finland---pasienter-presset-for-penger-1.15214710`. 224

[11] IBM. The 2020 cost of a data breach report explores financial impacts and security measures that can help your organization mitigate costs. Available from: "`https://www.ibm.com/security/data-breach`". 224

[12] LU, S., AND LYSECKY, R. Data-driven anomaly detection with timing features for embedded systems. *ACM Transactions on Design Automation of Electronic Systems (TODAES) 24*, 3 (2019), 1–27. 229

[13] MARTINS, A., AND ELOFE, J. Information security culture. In *Security in the information society*. Springer, 2002, pp. 203–214. 224

[14] NANDI, A., MANDAL, A., ATREJA, S., DASGUPTA, G. B., AND BHATTACHARYA, S. Anomaly detection using program control flow graph mining from execution logs. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (2016), pp. 215–224. 228

[15] RØSTAD, L., AND EDSBERG, O. A study of access control requirements for healthcare systems based on audit trails from access logs. In *22nd*

Annual Computer Security Applications Conference (ACSAC 2006), 11-15 December 2006, Miami Beach, Florida, USA (2006), IEEE Computer Society, pp. 175–186. 152, 201, 202, 217, 225, 226, 247

[16] SASSE, M. A., BROSTOFF, S., AND WEIRICH, D. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal 19*, 3 (2001), 122–131. 224

[17] STUDIAWAN, H., AND SOHEL, F. Performance evaluation of anomaly detection in imbalanced system log data. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (2020), IEEE, pp. 239–246. 235

[18] VERISON. Data breaches report. 2019, 2019. Available from: `https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf`. 199, 217, 224

[19] WHITMAN, M. E., FENDLER, P., CAYLOR, J., AND BAKER, D. Rebuilding the human firewall. In *Proceedings of the 2nd annual conference on Information security curriculum development* (2005), pp. 104–106. 2, 224

[20] YENG, P., WOLDAREGAY, A. Z., AND HARTVIGSEN, G. K-cusum: Cluster detection mechanism in edmon. 25, 217, 234, 249, 298

[21] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[22] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 11, 15, 22, 138, 200, 217, 224, 236, 273, 274, 404, 406, 407, 409, 414, 426, 442, 491, 498

[23] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 1, 2, 6, 10, 11, 15, 17, 23, 199, 217, 224, 274, 282, 404, 405, 406, 407, 409, 410, 414, 442, 443, 454, 457, 491, 498

[24] ZHANG, H., MEHOTRA, S., LIEBOVITZ, D., GUNTER, C. A., AND MALIN, B. Mining deviations from patient care pathways via electronic medical record system audits. *ACM Transactions on Management Information Systems (TMIS) 4*, 4 (2013), 1–20. 226, 227

[25] ZIEMNIAK, T. Use of machine learning classification techniques to detect atypical behavior in medical applications. In *2011 Sixth International Conference on IT Security Incident Management and IT Forensics* (2011), IEEE, pp. 149–162. 200, 201, 217, 227

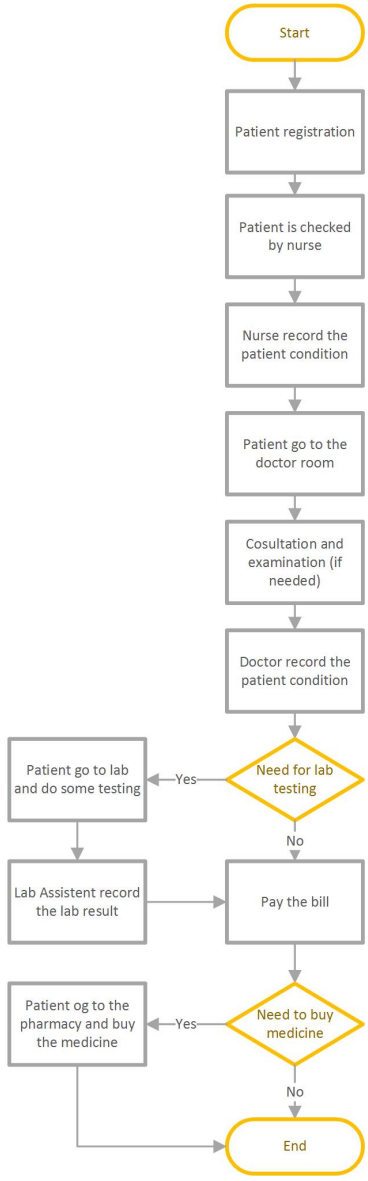


Figure 8.2: The Outpatients Department Flow

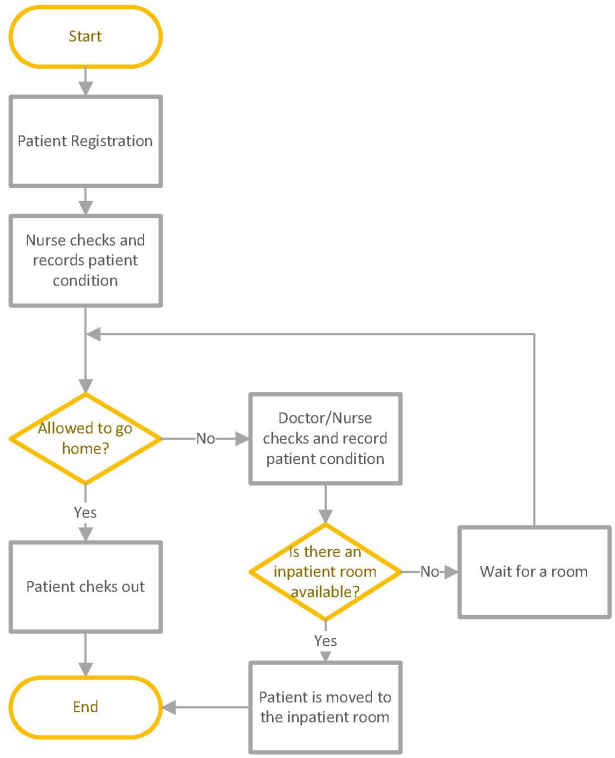
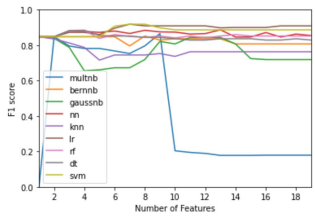


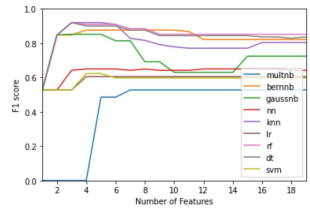
Figure 8.3: The Emergency Department Flow

		Predicted	
		Anomaly	Normal
Actual	Anomaly	TP	FN
	Normal	FP	TN

Figure 8.4: Confusion Matrix



(a) Result on Non-Normalised Data



(b) Result on Normalized Data (Min-Max)

Figure 8.5: F1-Score of Anomaly Detection with Number of Feature Variance.

2022 1st International Conference on AI in Cybersecurity (ICAIC) https://doi.org/10.1109/ICAIC53980.2022.9897055

Chapter 9

Analysing digital evidence towards enhancing healthcare security practice: The KID model.

2022 1st International Conference on AI in Cybersecurity (ICAIC)

Prosper K. Yeng, Muhammad A. Fauzi; Bian Yang and Sule Y. Yayilgan

Abstract

Due to emergency situations in healthcare, there is a requirement in electronic health records in various hospitals for emergency access known as ”Break-the-glass” or self-authorization. This is in compliance with the availability aspect of the information security (IS) principles. This requirement therefore, provides broad access to healthcare staff. Meanwhile internal users of Electronic health records (EHR) system such as the healthcare staff can exploit their legitimate broad access right to breach privacy and hence, the need to analyse the digital evidence of their logs towards enhancing privacy and security.

But, the lack of labelled data makes it challenging to efficiently assess the security practice of the users in a big data context. Therefore we developed a K-means iterative and discriminate model (KID model) towards identifying normal and abnormal security practice among healthcare staff with unlabelled logs of EHR of a typical hospital. The model was tested with real logs which captured all evidence of the healthcare staff’s login and logout transactions between 13 May 2014 and 17 April 2021. The data contains 933,508 sessions from 1,220 unique users in 2,623 unique days and these were anonymised.

The model was evaluated to be reliable with the Silhouette approach and it was used to determine abnormal and normal security practices. Some staff logged in for over three years without logout which is a huge security gap. Multiple sources of login sessions of the system administrator’s account was also detected. Other abnormal clusters also showed unusual patterns of long session duration and some healthcare staff such as doctors and nurses were averagely using one terminal in a day to create login and

logout sessions. Management could take measures to investigate into the cause of long session duration as that can be an opening for session hijacking. Also, the normal and abnormal behaviour which were detected in the study can be further assessed to be used for labelling data for supervised learning purposes.

9.1 Introduction

Digital evidence (DE) of healthcare staff in electronic health records (EHR) system, consists of the logs containing event recordings of the digital footprint of those who access the system. Due to privacy and security concerns, tracking and recording the evidence of accesses in EHR has become an essential requirement. For instance, the general data protection act of Ghana requires data controllers to maintain the integrity of personal data in their possession and control, by adopting the right technical and organizational measures to ensure unauthorized access, loss, damage and unauthorized processing of personal data [5]. Data controllers are also required to assess both internal and external risks to personal data and provide safeguards towards mitigation. Similarly, the code of conduct (Normen) based on the general data protection regulation (GDPR) together with the international organization for standardization for healthcare security (ISO/IEC 27799), has specified logging evidence of access to personal health information (PHI) as a security control clause [8, 6, 22]. Failure to implement logging of DE can be considered as a lack of due process which can result in heavy fines from the regulatory bodies, especially in data breach assessment scenarios. DE logging is therefore expected to be implemented in access control mechanisms in EHR systems. It is also required for data protection officers (DPO) to analyse the logs of DE towards safeguarding the privacy and security of personal health information (PHI).

Furthermore, since patient care path-ways are linked to accessing the patient PHI, broad access to PHI, known as "break-the-glass" (BTG) or "self-authorization" is required to be provided for the healthcare professionals. This is to ensure easy access of PHI, especially during emergency situations [8, 6, 14, 7]. It also fulfils the availability aspect of the confidentiality, integrity and availability (CIA) trait. Therapeutic events in healthcare have time sensitivity. When there are delays in providing healthcare, the patients' condition can worsen and in some situations (such as accidents), mortality occur if the necessary care is not provided at the right away. BTG mechanism in EHR enables healthcare workers to access patients' records without passing through the conventional processes of authorization. The effect is to provide easy access for the healthcare staff to provide therapeutic measures to patients in a timely manner. The issue with this mechanism is that BTG increases the security and privacy vulnerability of the personal health infor-

mation if the healthcare workers tend to be the direct internal threat actors [14]. Broad access through the BTG mechanism means that healthcare personnel could access patients' records for other reasons other than healthcare purposes. For instance, there have been various reports on PHI snooping, which violates the principle of accessing healthcare records for therapeutic purposes [14, 7, 11].

Various studies opined that healthcare staff tend to share their authentication criteria such as usernames and passwords, and therefore act as serious threat actors [14]. In a scenario where the credentials of a healthcare worker who has broad access to patients' records, is shared with colleagues or it happens to fall into the hands of an external threat actor, the security can be hugely impacted [21]. To reduce such risks, the code of conduct requires not only the tracking and recording of DE but to have the possibility to analyze logs using analysis tools with the aim of detecting breaches. The general objective of this study is to therefore analyse real DE that has been logged in the EHR of a hospital that has digitized its healthcare operations. This will enable the health facility to know if there are potential privacy and security risks of data breaches and how these can be mitigated.

9.1.1 Problem statement, scope and contribution

In principle, healthcare data need to be strictly accessed for therapeutic reasons by healthcare staff [13, 23, 18]. Furthermore, security policies require end-users to comply with password management security practices by not sharing the same authentication system. Healthcare organizations such as a hospital is therefore required to identify and distinguish normal security practice from abnormal accesses towards enhancing data privacy and security. This can be challenging in practice with manual verification due to huge access logs [13] of digital evidence. Also, in situations where there is no labelled data, supervised method in machine learning can not be adopted to examine for privacy and security gaps in DE [21, 19, 20].

In fact, a related study [14] ruled out unsupervised methods such as clustering as a choice to identify abnormal security practices in DE. They argued that abnormal patterns tend to be the minority in big data logs which get classified into normal patterns. In this work, we proved that the k-means clustering method can be used to assess abnormal behaviour when it is combined with the discriminate-iterative approach. To this end, we hypothesized that abnormal security and privacy practices can be detected by using unsupervised machine learning methods. So we designed an iterative clustering model with a discriminant approach for detecting abnormal security practices in healthcare. The model was further assessed with real digital evidence of logs from a typical hospital.

9.1.2 Related work

Various studies have tried to provide machine learning-based solutions towards analyzing EHR logs for detecting atypical behaviour. For instance, [21, 19, 20] simulated EHR logs to demonstrate how DE can be analysed for abnormal security practice. The study, therefore, provided a framework and compared various supervised machine learning methods.

Zheng et al developed a model (called patient flow-based anomaly detection) to detect abnormal behaviour [24]. The model was based on their opinion that patient care follows a structured workflow and therefore, the access of the patient records can be aligned with the progression of the patient along the pathway. The sequence of access to the patient records can be represented in a graph. The purpose of accesses represents the features of the patient record accesses linked together on the graph. Electronic health records (EHR) logs were used in this study. A baseline of patient flow was established and a scoring model was developed to assess the extent to which various accesses deviate from the historical pattern of the flow of the patient in the patient care path. The model uses a directed graph of the features of interactions between the healthcare staff and the patient including roles of users, their reason of access, patient location. A smaller proportion of accesses were detected to have deviated greatly from their established patient-flow path. In related work, Cosatante et al proposed a data loss prevention and detection framework [16]. The framework uses a hybrid of signature-based and anomaly-based solutions for detection and preventing unauthorised access. The anomaly-based model is incorporated with normal user behaviour for it to be able to detect abnormal user accesses. The abnormal behaviours which are flagged are verified. The certified malicious actions are updated in the signature-based engine that is then used for preventing unauthorised accesses [3]. The prevention module adopted a rule-based approach and the module was first validated with synthetic data from the healthcare management system. The normal behaviour of the healthcare users was simulated over 15 days. The experimental results showed that the algorithms were able to prevent unauthorised data leakage.

Essentially, the contribution of [24, 16] helped in the detection of abnormal accesses however, a supervised learning approach was used. This limits the use of algorithms for detecting abnormal security practices without labelled data.

In a similar way, following the privacy and security concerns of patients, Boddy et al developed a human-in-the-loop machine learning (HILML) algorithm to detect unauthorised accesses in electronic health records logs [1]. The algorithm also incorporated a model called density-based outlier detection (DBOD). DBOD assesses the density around an object and compares it to the densities of its peers. If the density of that object is comparatively lower, then it is considered an outlier [12]. Furthermore, a related

study assessed six anomaly detection categories including clustering-based, nearest-neighbour-based, classification, statistical spectral and information theoretical-based for their suitability towards assessing abnormal security practice. However, none of these was found suitable to meet its study requirement [14]. The study was constrained with unlabeled data, a transparent retracing of abnormal behaviour and a lack of details in data files for ruled-based related categories. Eventually, a scoring approach was settled on because it met the study requirement such as traceback and easy integration into the input and output system of the hospital.

All these approaches aimed towards contributing knowledge for detecting abnormal security practice in healthcare but K-means clustering, combined with iteration and discriminate method has not been modelled for detecting abnormal security and privacy practice in DE of EHR logs and therefore solidifies this piece of work as a novelty.

9.1.3 K-means clustering combined with iteration and discriminate approach

Clustering is a method used to divide large data into a set of groups [17]. Each group differs from the other but similar data points are found within the same group. The most popular type of clustering includes K-means and hierarchical clustering. Hierarchical clustering is a bottom-up approach where numerous clusters are initially generated [2]. Based on the characteristics of the clusters, the most similar clusters are aggregated and the process is repeated until a single cluster is formed. This approach is not compatible with our goal for detecting abnormal security practices. Grouping similar clusters will not showcase the few abnormal security practices in the big data context [14]. With K-means clustering [10], the number of (K) is first determined. This is followed by determining the centroids of the K and assigning the various points to the nearest cluster centroid. The process is repeated by determining new centroids and assigning near data points to the centroids until a centroid of new clusters remains unchanged.

This approach was explored with iteration and discriminated approach towards identifying abnormal security practice in the DE.Elbow method was used for determining the best K as it is the most common method often used with K-means. The Elbow method [4] determines the best k by first computing for the average distance between a cluster centroid and its data points with various numbers of varying K. It calculates the sum of the square of the points as the distance and further calculates the average distance. When the value of K is 1, the sum of the square value within-cluster will be high but as the value of K increases, the sum of the square value decreases. A graph is plotted between K-values and within-cluster average distances to obtain the k value. The graph is assessed for the best K at the

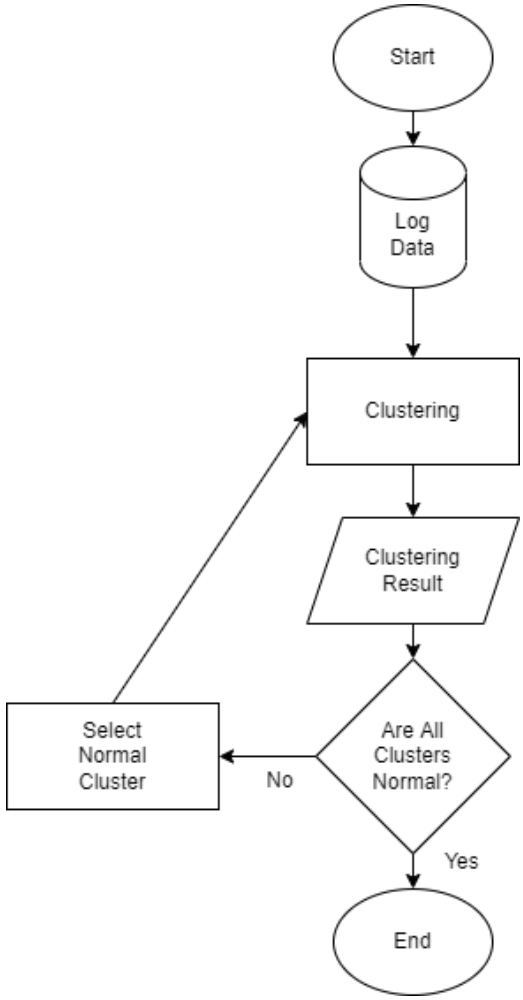


Figure 9.1: Iterative Clustering Steps.

point, where the graph decrease abruptly.

Anonymised log data were provided from a hospital information system in Ghana. The log system captured all evidence of the healthcare staff's login and logout transactions between 13 May 2014 and 17 April 2021. As displayed in Table9.2, the data contains 933,508 sessions from 1,220 unique users on 2,623 unique days. A session is a time between login and logout of a unique user.

Furthermore, the number of computers used for the sessions are 407 with

1,367 unique internet protocol (IP) addresses. The users who accessed the hospital information system were from several professions. Nurses and doctors were the professions with the most users, as depicted in Table 9.3with 671 and 312 users respectively. The login and logout sessions were accumulated in each day and their statistics such as number of logins with manual log out, number of logins without manual log out, session length and their respective averages and percentiles were computed and used in the clustering. The baseline of a normal cluster was assumed to have an average of 8 hours of session time per user and that cluster should have a comparatively higher number of sessions because it was assumed that normal behaviour in a typical hospital will have the majority of activities in the logs [14]. An iterative clustering was conducted on the data as displayed in Figure 9.1 and in figure9.5. In each iteration, the data were clustered into some number of clusters. Abnormal clusters were discriminated against and were not added in the next round of iteration. Clusters with normal or near-normal cumulative sessions duration (e.g. the lowest cumulative sessions duration) were further analyzed in the next iteration. The objective of the iteration was to see whether all of the data in the normal cluster has normal cumulative sessions duration. The iteration will stop when all of the data in the normal cluster has a normal cumulative sessions duration.

In terms of evaluation, Silhouette method was adopted as it is the common method for assessing a cluster in k-means [15]. It involves the assessment for cohesion and separation which are then used to determine the Silhouette coefficient. In cohesion, the average of the distances of a data point to its neighbours within a cluster are computed(ai). Whereas in separation, the average distance between the data point and other data points in its next closest cluster is computed (bi). The average distance within the cluster (ai) is less than that of the data point and its counterparts in another cluster (bi). The silhouette coefficient is then calculated for all the points in the clusters and plot the silhouette graph. The graph is plotted between -1 to 1, where the silhouette coefficient closer to 1 is better as the silhouette coefficient closer to 0 is the worst-case scenario.

9.2 Analysis and findings

The KID model was evaluated and the findings are shown in table 9.1.

The Silhouette Coefficient [9] is expected to be in the range of -1 to 1. A score of one means that the clusters are well separated but a score of 0 implies that the clusters are overlapping whiles a score of fewer than 0 means that data points belonging to clusters may be incorrect. Our results showed that the Silhouette coefficients are all within the range of 0.496 to 0.997 suggesting that, our clusters are well separated.

The Figure 9.2 shows that out of the 933,508 login transactions, 73% of

Table 9.1: Silhouette Coefficient.

Clustering Step	Silhouette Coefficient
1	0.997
2	0.983
3	0.526
4	0.496

Table 9.2: Log data characteristic.

Characteristic	#
Number of sessions	933,508
Number of unique users	1,220
Number of unique days	2,623
Number of unique terminal IPs	1,367
Number of unique terminal names	407

them (676,801) were through a manual logout action. Meaning that those healthcare workers consciously log-out their session after a login. Meanwhile, the other 27% (256,707) were not followed by a manual logout by the user so that the system automatically logout the user. Furthermore, as displayed in Table 9.4, the average session duration of the 676,801 logins with logout transactions is 3.16 hours. Meanwhile, the shortest session duration was 0 hours and the longest is 28,847.25 hours. As shown in Figure 9.3, most of the records have session duration between 0-1 hour. The Number of Sessions is declining along with the number of hours. The minimum number of Sessions were those with a session duration of 7-8 hours (3,390 records). Meanwhile, there were 10,182 records with a session duration of more than 8 hours. Furthermore, according to Figure 9.4, only 5% (59) of users always manually logout after login. The other 95% (1161) did not manually logout after login in at least one time.

To analyze the data, we grouped the logs data into 24-hour cumulative session blocks for each user so that an instance represents the cumulative sessions of a user in one day. As a result, 275,134 cumulative sessions were extracted from the logs. On average, there were 2.64 sessions for each user in one day. According to Table 9.5, most users only use 1 terminal to login in a day. The number of sessions was declining along with the number of terminals used by one user in one day. However, there are some days in which some users used more than 10 terminals to access the system in one day. Based on Figure 9.5, most of the accesses with a lot of terminals were conducted by System Administrators or System Developers.

Afterwards, the cumulative sessions instances were then transformed into features for the clustering process. Table 9.6 shows the features extracted from the cumulative session. Subsequently, the data were clustered

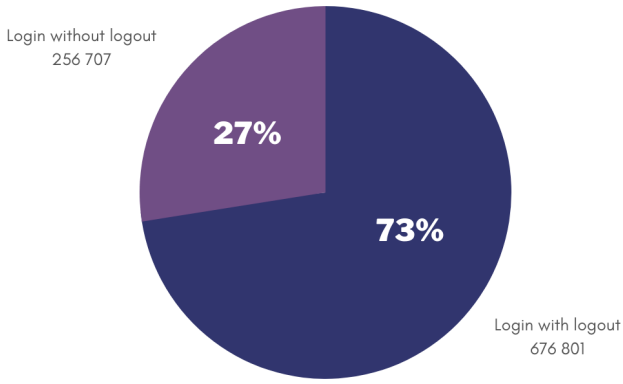


Figure 9.2: Login characteristic.

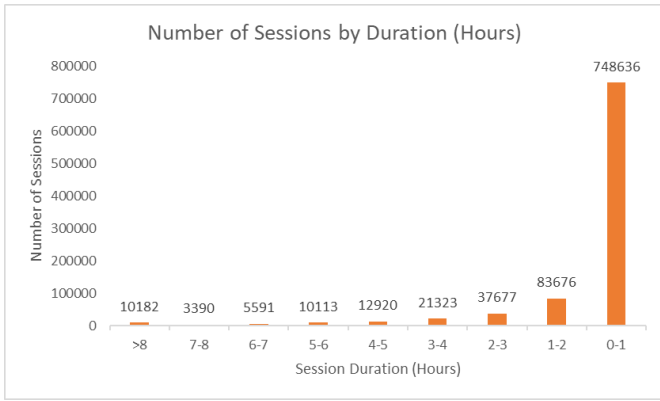


Figure 9.3: Number of Sessions by Session Duration.

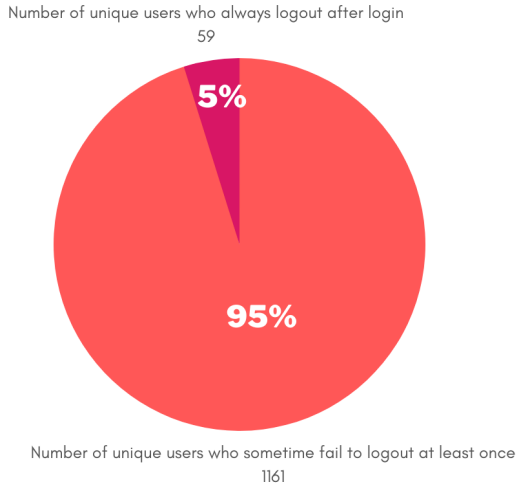


Figure 9.4: User login and logout percentage.

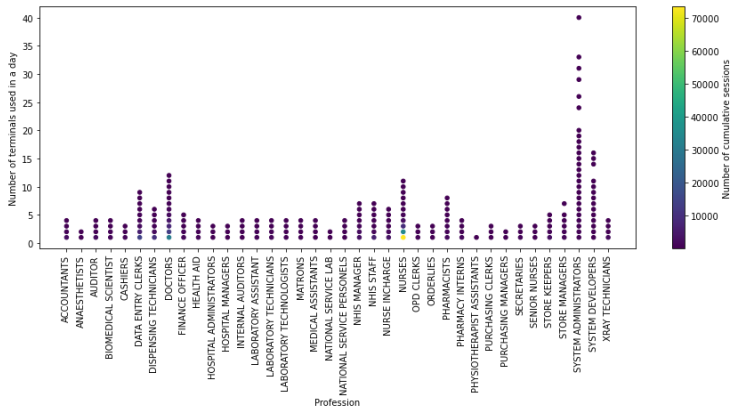


Figure 9.5: Number of Terminals Used by Profession.

Table 9.3: User Profession.

Profession	#
ANAESTHETISTS	1
INTERNAL AUDITORS	1
MATRONS	1
NATIONAL SERVICE LAB	1
PURCHASING CLERKS	1
PURCHASING MANAGERS	1
SYSTEM DEVELOPERS	1
AUDITOR	2
HOSPITAL ADMINISTRATORS	2
HOSPITAL MANAGERS	2
OPD CLERKS	2
PHYSIOTHERAPIST ASSISTANTS	2
CASHIERS	3
LABORATORY TECHNOLOGISTS	3
ORDERLIES	3
PHARMACISTS	3
MEDICAL ASSISTANTS	4
SECRETARIES	4
SENIOR NURSES	4
STORE MANAGERS	4
SYSTEM ADMINISTRATORS	4
BIOMEDICAL SCIENTIST	5
STORE KEEPERS	5
XRAY TECHNICIANS	5
FINANCE OFFICER	6
NATIONAL SERVICE PERSONNEL	6
LABORATORY ASSISTANT	8
PHARMACY INTERNS	8
NHIS MANAGER	9
NHIS STAFF	9
ACCOUNTANTS	10
HEALTH AID	11
LABORATORY TECHNICIANS	13
NURSE INCHARGE	14
DISPENSING TECHNICIANS	22
DATA ENTRY CLERKS	57
DOCTORS	312
NURSES	671

Table 9.4: Login with logout data statistic.

Statistic	Session Duration (hour)
mean	3.16
std	118.49
min	0.00
25 %	0.09
50 %	0.34
75 %	1.12
max	28,847.25

Table 9.5: Number of Cumulative Sessions by Number of Terminals Used.

Number of Terminal Used in One Day	Number of Cumulative Sessions
1	168488
2	68510
3	22861
4	9035
5	3617
6	1482
7	630
8	294
9	108
10	57
11	15
12	7
13	6
14	3
15	5
16	3
17	1
18	2
19	1
20	2
24	1
26	1
29	2
31	1
33	1
40	1

into various clusters using the K-means method.

Based on the elbow method displayed in Figure 9.6, the first clustering used 7 clusters and the result statistics can be seen in Table 9.7. The cluster-

Table 9.6: Clustering features.

Feature	Details
NumberOfSessions	The number of sessions of the user in 24-hour
NumberOfLoginWithoutLogout	The number of login without manual logout sessions of the user in 24-hour
NumberOfLoginWithLogout	The number of login with manual logout sessions of the user in 24-hour
SessionDurationMean	The average session duration of the user in 24-hour
SessionDurationMin	The minimum session duration of the user in 24-hour
SessionDurationMax	The maximum session duration of the user in 24-hour
SessionDurationStd	The standard deviation of session duration of the user in 24-hour
CumulativeSessionDuration	The sum of session duration of the user in 24-hour
SessionDurationMedian	The median of session duration of the user in 24-hour
NumberOfTerminal	The number of terminal used by the user in 24-hour
NumberOfIP	The number of terminal IP used by the user in 24-hour
PercentLoginWithoutLogout	The percentage of login without manual logout transactions of the user in 24-hour
PercentLoginWithLogout	The percentage of login with manual logout transactions of the user in 24-hour
Profession	The profession of the user

ing result shows that the main difference between each cluster is the length of the access duration. The average sessions duration in Cluster 0 is only 1.58 hours. Meaning that when the users logged in, they logged out after an average of 1.58 hours. In contrast, the duration of the average session in Cluster 1, 2, 3, 4, 5, and 7 are thousand hours. It means that when the users logged in, they never logged out after many days. Furthermore, the average cumulative sessions duration in a day in Cluster 0 is only 3.25 hours. It means that in one day, the users only access the system for 3.25 hours on average. For the rest of the cluster, it seems that in one day the users' account is always active 24 hours on the system. Based on this data, it means that Cluster 0 shows a normal activity but the rest of the cluster show an anomaly in which the users never logged out for a long time. However, we can see that the number of records in Cluster 0 is 274854, far higher than the

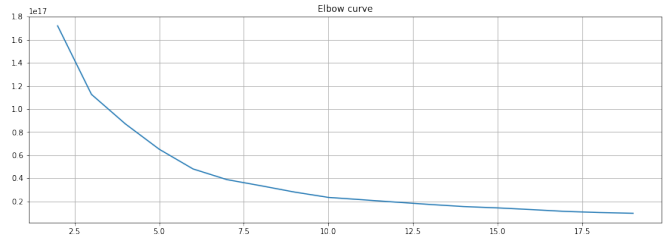


Figure 9.6: Elbow Method for first iteration.

rest of the cluster. Therefore, the normal activities are still the majority and anomaly is the minority.

Table 9.7: First Step Clustering result statistic.

Cluster	Cluster 0	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6
Number of Sessions	274854	10	36	11	181	39	3
Average Number of Sessions	3.39	1.20	4.11	2.55	2.27	1.28	2.67
Average Session Duration per Transaction (Hour)	1.58	12330.60	2248.10	5777.21	1348.96	5179.06	10120.01
Cumulative Session Duration (Hour)	3.25	13632.82	6985.82	14144.62	2206.79	5775.60	25048.01
Average Number of Terminal	1.62	1.00	1.94	1.45	1.23	1.05	1.33
Average Number of IP	1.67	1.00	1.94	1.45	1.28	1.08	1.33
Average Percentage Login Without Logout (%)	26.08	5.00	4.10	0.00	4.43	3.33	0.00
Average Percentage Login With Logout (%)	73.92	95.00	95.90	100.00	95.57	96.67	100.00

Furthermore, we analyzed data from Cluster 0 by conducting the second K-Means clustering to group the data. The objective is to see whether all of the data in Cluster 0 is normal. Based on the elbow method in Figure 9.7, the optimal number of clusters is seven. The second clustering result statistics can be seen in Table 9.8. Based on the results, not all of the data in Cluster 0 from the first iteration is normal. There are several data that has cumulative sessions duration of more than 8 hours. Cluster 0 has the most members (274,467 instances) and has a normal average cumulative sessions duration of 2.59 hours. It means that Cluster 0 can be considered normal. Meanwhile, the other clusters' average cumulative sessions duration are hundred

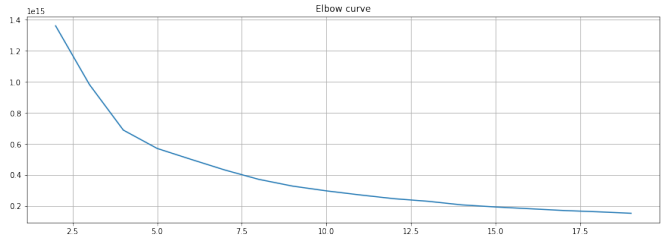


Figure 9.7: Elbow Method for the second iteration.

of hours which indicates an anomaly. Therefore, we will further analyze Cluster 0 for the third iteration.

Table 9.8: Second Step Clustering result statistic.

Cluster	Cluster 0	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6
Number of Sessions	274467	75	31	25	42	32	182
Average Number of Sessions	3.39	3.51	1.13	5.92	1.55	3.56	3.41
Average Session Duration per Transaction (Hour)	1.28	197.58	653.24	216.11	295.58	354.06	90.55
Cumulative Session Duration (Hour)	2.59	582.81	709.22	1131.08	362.00	1040.01	219.51
Average Number of Terminal	1.62	1.65	1.00	1.72	1.10	1.25	1.51
Average Number of IP	1.67	1.69	1.00	1.80	1.10	1.25	1.55
Average Percentage Login Without Logout (%)	26.11	3.68	1.61	2.00	9.33	2.86	6.97
Average Percentage Login With Logout (%)	73.89	96.32	98.39	98.00	90.67	97.14	93.03

Based on the elbow method in Figure 9.8, the optimal number of cluster for the third iteration is seven. The third clustering result statistics can be seen in Table 9.9. Based on the results, not all of the data in Cluster 0 from the second iteration is normal. There are several data that has a cumulative sessions duration of more than 8 hours. Cluster 0, 2, 5, and 6 have a normal average cumulative sessions duration in a day (less than 8 hours). It means that these clusters can be considered normal. Meanwhile, Cluster 1, 3, and 4 can be considered anomalies based on the average cumulative

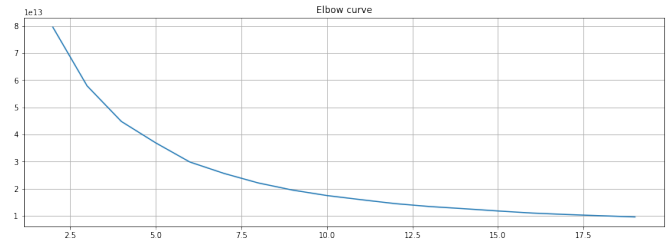


Figure 9.8: Elbow Method for the third iteration.

sessions duration in a day that is more than 8 hours. For the next iteration, we choose the normal cluster. Since we have several normal clusters and we have to select only one cluster, we choose Cluster 5, the one with the minimum average cumulative sessions duration. The cluster with the minimum average cumulative sessions duration was selected because we want to choose a cluster that has the highest chance to have all of the data in the cluster are normal.

Table 9.9: Third Step Clustering result statistic.

Cluster	Cluster 0	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6
Number of Sessions	72943	4114	16767	2931	221	153791	23700
Average Number of Sessions	4.37	4.54	1.38	1.35	3.65	2.93	4.86
Average Session Duration per Transaction (Hour)	1.34	5.60	5.46	12.74	29.68	0.28	2.24
Cumulative Session Duration (Hour)	3.17	17.27	5.76	13.41	60.94	0.57	7.26
Average Number of Terminal	1.88	1.94	1.07	1.09	1.67	1.49	2.12
Average Number of IP	1.94	1.97	1.08	1.10	1.74	1.53	2.17
Average Percentage Login Without Logout (%)	19.57	11.60	11.59	10.03	12.46	33.73	11.67
Average Percentage Login With Logout (%)	80.43	88.40	88.41	89.97	87.54	66.27	88.33

For the fourth iteration, seven is selected as the number of cluster based on the elbow method in Figure 9.9. The fourth clustering result statistics can be seen in Table 9.10. Based on the results, all of the data in Cluster 5 from

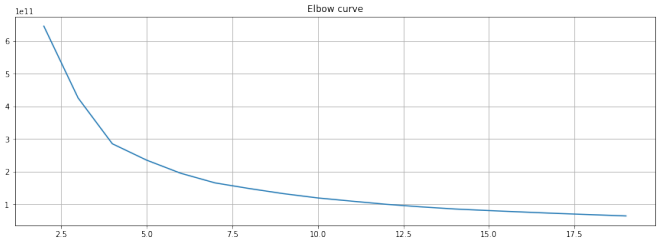


Figure 9.9: Elbow Method for fourth iteration.

the third iteration are normal. All of the clusters have a normal average cumulative sessions duration in a day (less than 8 hours). It means that all of these clusters can be considered normal. Since all of the data are normal at this point, the iteration finish. Finally, we evaluated the clustering result using Silhouette Coefficient. Table 9.1 shows that the Silhouette Coefficients of the first and second clustering results are good but the third and fourth clustering results are quite poor. The data in the first and second iteration are still very diverse so that they are easy to be separated while the data in the third and last clustering are very similar.

Table 9.10: Fourth Step Clustering result statistic.

Cluster	Cluster 0	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6
Number of Sessions	19663	60171	9531	11022	30746	9600	13058
Average Number of Sessions	4.75	1.90	1.95	3.61	2.94	7.16	1.95
Average Session Duration per Transaction (Hour)	0.31	0.03	1.04	0.60	0.22	0.38	0.60
Cumulative Session Duration (Hour)	0.99	0.05	1.11	1.46	0.39	1.94	0.66
Average Number of Terminal	2.01	1.20	1.18	1.71	1.50	2.65	1.19
Average Number of IP	2.08	1.22	1.21	1.77	1.54	2.75	1.22
Average Percentage Login Without Logout (%)	18.19	53.64	27.64	21.57	19.67	16.27	26.08
Average Percentage Login With Logout (%)	81.81	46.36	72.36	78.43	80.33	83.73	73.92

9.3 Discussion and study implication

While "break-the-glass" (BTG) requirement in healthcare, complies with the availability objective of the CIA trait, it can inadvertently undermines the confidentiality and integrity aspects of information security. Because internal threat actors are likely to exploit their legitimate access to breach privacy and security in healthcare through the BTG window. This study therefore developed an model (the KID model) and used it to analysed the logs of healthcare staff using K-means, iterative and discriminate approach. The goal was towards identifying irregular security practices towards enhancing the privacy and security of EHRs.

Highlights of our findings showed abnormalities that threaten privacy and security. For instance, from the data analysis, the longest session duration at a time was 28,847.25 hours (1201 days or 40months or 3.3 years) by a user. This action was performed by a healthcare administrative officer. This is a huge anomaly in the sense that average session duration in a typical hospital should be 8 hours. Moreover, various clusters showed anomalies, for example in the first iteration, cluster 1 to cluster 6 each has average session time and cumulative session in thousands of hours with relatively fewer sessions as shown in the Table 9.7. This could mean that many users are using the same user accounts which therefore increases the session duration. Even if the personnel worked on double shift, the maximum session duration should be 16 hours. For a session duration to run into years implies that unauthorised persons can ride on the already login session to illegally access data and thereby compromising the confidentiality, integrity and availability (CIA) of the data. The obvious question will be that how did it happen in the first place? Why did the system fail to logout this user to prevent possible session hijacking? Such outliers need to be investigated towards enhancing security.

Also, there were 168,488 cumulative user sessions in a day that used only one term as shown in table9.5. Furthermore, from Figure 9.3, there were around 70000 and 40000 cumulative sessions from nurses and doctors that used only one terminal in a day respectively in their assesses to the EHR. Furthermore, around 50000 cumulative sessions were generated by nurses by using two terminals in a day while doctors used two terminals in a day to generate about 20000 cumulative sessions. However, some users used more than two terminals in a day. Users that used many terminals in a day can be interpreted that they always move to several places for their work. Based on Figure 9.5, IT-related users are those that used many terminals in a day. Generally, it can be interpreted to be quite normal for them to work on many different computers in a day since they may need to check or fix something on many computers in a day. However, while this is inclusive of a normal security practice, there is also a likelihood that unauthorised users can use the admin credentials to login from multiple terminals.

Regarding adherence to login and logout behaviour of users, 75% complied with that policy but 27% failed to always logout after work. Clearly, the majority of the users are complying with the login and lout practice however, the few 27% could thwart the efforts of the majority. Because security malpractices could happen within the few who do not follow the policy. In any case, it is better to have a few proportions of the staff in the non-compliance category instead of the reverse. Better incentive could be used to improve on the login/logout practice of the user. Using the iterative approach, this study guided in determining the gaps in security practice by showcasing normal security practice from abnormal practices. For instance, there are some staff who log in for over three years without logout which is a huge security gap. Management could take measures to prevent such vulnerabilities. Secondly, the normal behaviour which was identified in the last iteration in table 9.10 can be used to label the data for supervised learning purposed towards detecting real-time abnormal behaviour in the electronic healthcare records.

9.3.1 Conclusion

Observing security practices in electronic health records logs is paramount. However, it is challenging to use machine learning methods to analyse the logs when labelled data are not available[21]. Therefore, we developed an iterative discriminant K-means clustering model which was used to assess the security practice of healthcare staff in real digital evidence of the accesses of healthcare staff. The clusters were evaluated with the Silhouette method. The model was then used to detect abnormal security practice from the entire logs. Some users were found to be logging onto many computers which can be a vulnerability for user authentication sharing. These findings can be used to investigate abnormal security practices which were identified in this study. Future works will explore spatial-temporal approach towards detecting overlapping of session times from multiple log in sources. Additionally, since abnormal does not mean the occurrence of breaches, future works will be validating the abnormal practices to substantiate data breaches.

9.4 Bibliography

[1] BODDY, A. J., HURST, W., MACKAY, M., AND EL RHALIBI, A. Density-based outlier detection for safeguarding electronic patient record systems. *IEEE Access 7* (2019), 40285–40294. 52, 55, 248

[2] BRIDGES JR, C. C. Hierarchical cluster analysis. *Psychological reports 18*, 3 (1966), 851–854. 249

[3] COSTANTE, E., DEN HARTOG, J., PETKOVIĆ, M., ETALLE, S., AND PECHENIZKIY, M. A white-box anomaly-based framework for database leakage detection. *Journal of Information Security and Applications 32* (2017), 27–46. 52, 53, 55, 248

[4] CUI, M., ET AL. Introduction to the k-means clustering algorithm based on the elbow method. *Accounting, Auditing and Finance 1*, 1 (2020), 5–8. 249

[5] DATA PROTECTION COMMISSION. The data protection act, 2012 (act 843),, 2018. Available from: "https://www.dataprotection.org.gh/index.php/data-protection/data-protection-acts-2012". 52, 55, 246

[6] FOR EHEALTH, D. The code of conduct for information security and data protection in the healthcare and care services, 2020. Available from: "https://www.ehelse.no/normen/documents-in-english". 52, 246

[7] GORMAN A., S. A. Tsix people fired from cedars-sinai over patient privacy breaches. la times., 2013. Available from: "https://www.ehelse.no/normen/documents-in-english". 52, 246, 247

[8] ISO. Health informatics information security management in health using iso/iec 27002, 2016. Available from: "https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en". 52, 53, 246

[9] KUMAR, A. Kmeans silhouette score explained with python example, 2018. Available from: "https://dzone.com/articles/kmeans-silhouette-score-explained-with-python-exam". 251

[10] LIKAS, A., VLASSIS, N., AND VERBEEK, J. J. The global k-means clustering algorithm. *Pattern recognition 36*, 2 (2003), 451–461. 249

[11] MENON, A. K., JIANG, X., KIM, J., VAIDYA, J., AND OHNO-MACHADO, L. Detecting inappropriate access to electronic health records using collaborative filtering. *Machine learning 95*, 1 (2014), 87–101. 52, 53, 247

[12] RANJAN, K. G., AND PRUSTY, B. R. A detailed analysis of adaptive kernel density-based outlier detection in volatile time series. In *Machine Learning, Advances in Computing, Renewable Energy and Communication*. Springer, 2022, pp. 359–369. 52, 53, 55, 248

[13] RØSTAD, L., AND EDSBERG, O. A study of access control requirements for healthcare systems based on audit trails from access logs. In *22nd Annual Computer Security Applications Conference (ACSAC 2006), 11-15*

December 2006, Miami Beach, Florida, USA (2006), IEEE Computer Society, pp. 175–186. 152, 201, 202, 217, 225, 226, 247

[14] STARK, B., GEWALD, H., LAUTENBACHER, H., HAASE, U., AND RUFF, S. Misuse of 'break-the-glass' policies in hospitals: Detecting unauthorized access to sensitive patient health data. *International Journal of Information Security and Privacy (IJISP) 12*, 3 (2018), 100–122. 52, 246, 247, 249, 251

[15] THINSUNGNOENA, T., KAOUNGKUB, N., DURONGDUMRONCHAIB, P., KERDPRASOPB, K., AND KERDPRASOPB, N. The clustering validity with silhouette and sum of squared errors. *learning 3*, 7 (2015). 251

[16] WHO. Attacks on health care in the context of covid-19. 2020 30 july 2020, 2021. Available from: `https://www.who.int/news-room/feature-stories/detail/attacks-on-health-care-in-the-context-of-covid-19`. 52, 55, 248

[17] YENG, P., WOLDAREGAY, A. Z., AND HARTVIGSEN, G. K-cusum: Cluster detection mechanism in edmon. 25, 217, 234, 249, 298

[18] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[19] YENG, P. K., FAUZI, M. A., AND YANG, B. Comparative analysis of machine learning methods for analyzing security practice in electronic health records' logs. In *2020 IEEE International Conference on Big Data (Big Data)* (2020), IEEE, pp. 3856–3866. 22, 23, 25, 247, 248

[20] YENG, P. K., FAUZI, M. A., AND YANG, B. Workflow-based anomaly detection using machine learning on electronic health records' logs: A comparative study. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)* (2020), IEEE, pp. 753–760. 22, 23, 247, 248

[21] YENG, P. K., NWEKE, L. O., YANG, B., FAUZI, M. A., AND SNEKKENES, E. A. Artificial intelligence–based framework for analyzing health care staff security practice: Mapping review and simulation study. *JMIR Medical Informatics 9*, 12 (2021), e19250. 15, 22, 23, 247, 248, 263

[22] YENG P, FAUZI MA, S. L., AND B, Y. Legal aspects of information security requirements for healthcare in three countries: A scoping review as a benchmark towards assessing healthcare security

practices. *JMIR Hum Factors* (2022). Available from: https://humanfactors.jmir.org/2022/0/e0/. 7, 15, 246, 405

[23] YENG, PROSPER KANDABONGEE AND NWEKE, LIVINUS OBIORA AND WOLDAREGAY, ASHENAFI ZEBENE AND YANG, BIAN AND SNEKKENES, EINAR ARTHUR. Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. In *Proceedings of SAI Intelligent Systems Conference* (2020), Springer, pp. 1–18. 11, 19, 23, 200, 201, 202, 217, 247

[24] ZHANG, H., MEHOTRA, S., LIEBOVITZ, D., GUNTER, C. A., AND MALIN, B. Mining deviations from patient care pathways via electronic medical record system audits. *ACM Transactions on Management Information Systems (TMIS) 4*, 4 (2013), 1–20. 52, 55, 58, 248

Part III

Phishing attack and defense simulation

Chapter 10

Investigation into Phishing Risk Behaviour among Healthcare

MDPI: Information 2022, 13, 392

Prosper K. Yeng, Muhammad A. Fauzi, Bian Yang and Peter Nimbe

Abstract

A phishing attack is one of the less complicated ways to circumvent sophisticated technical security measures. It is often used to exploit the psychological and other factors of human users to succeed in social engineering attacks including ransomware. Guided by the state of the arts in a phishing simulation study in healthcare and after deeply assessing the ethical dilemmas, an SMS-based phishing simulation was conducted among healthcare workers in Ghana. The study adopted an in-the-wild study approach alongside quantitative and qualitative surveys. From the state-of-the-art studies, the in-the-wild study approach was the most commonly used method as compared to laboratory-based experiments and statistical surveys because its findings are generally reliable and effective. The attack results also showed that 61% of the targeted healthcare staff were susceptible, and some of the healthcare staff were not victims of the attack because they prioritized patient care and were not susceptible to the simulated phishing attack. Through structural equation modelling, the workload was estimated to have a significant effect on self-efficacy risk (r = 0.5, p-value = 0.05) and work emergency predicted perceived barrier in the reverse direction at a substantial level of r=-0.46, p-value=0.00. Additionally, Pearson's correlation showed that perceived barrier was a predictor of self-reported security behaviour in phishing attacks among healthcare staff. As a result, various suggestions including workload balancing extra layer of security controls in emergency departments and better security training were suggested to enhance staff's conscious care behaviour.

10.1 Introduction

Digitization refers to a holistic transformation of different sectors by adopting IT systems [56, 23]. The systems that are commonly used in the transformation include software applications, networks and hardware systems. This has been an ongoing course of action in the eHealth space, such as electronic health records (EHR), medical devices, decision support, and telemedicine among others. The recent COVID-19 has expedited the adoption rate and expanded the use of information communication technology (ICT) in the healthcare sector. The World Health Organization (WHO) confirmed this by indicating that there has been a tremendous increase in the use of mobile devices such as smartphones, tablets, embedded devices [60, 90] and laptops for self-management of healthcare, diagnosis, treatment, and disease surveillance [93].

Countries in Africa such as Ghana are not left out in the digitization drive in healthcare. Many healthcare facilities have adopted various kinds of ICT systems [2, 62, 9] including EHR to improve their healthcare delivery. The major threat in digitization relates to issues of cyber-security, especially the human aspect of information security.

Verizon [87] recently reported that human factors across the globe, accounted for a woefully 85% of the cyber-security incidents in 2020 , suggesting that, the human element is now the leading targeted mode of entry into healthcare systems.

According to Healthcare IT News [54], healthcare systems are ideal destinations for cyber criminals to launch ransomware attacks because healthcare provision is associated with time-sensitivity and urgency when accessing patient records especially during an emergency. This creates a sense of urgency forces for management to pay a ransom in ransomware attack scenarios in order to rescue data. Furthermore, there are many human vulnerabilities in healthcare that can enable attackers to gain illegitimate access to systems. For instance, the healthcare environment consists of people (staff, end users, developers, etc), working under busy and intensive conditions that can compel them to unintentionally click on malicious links or miss security measures. Most ransomware attacks start with the human as they present the main vulnerability in the hospital. This observation was supported by Chernyshev et al, who identified ransomware to be the most common type of malware in use, of which phishing was the most popular technique often used in data breaches in healthcare [20]. In a ransomware attack, criminals can encrypt data or cause a denial of service and demand for ransom to be paid before releasing the service [80]. Phishing methods are often used and it involve sending a malicious message to the targets that aimed to deliver payload into the IT system with the anticipation that at least a one of them would become victims. It is one of the easier ways to circumvent sophisticated technical security measures by exploiting psychological factors of the

human elements to gain unauthorised access. The mode of communication that is often used to lure targets includes social engineering-based phishing such as email, SMS (smishing), and voice (vishing) communication. Social engineering-based phishing attacks include deceptive, spear, and whaling approaches. Deceptive phishing involves targeting a larger group of persons, spear phishing targets specific organisations or groups of people and the whaling approach targets a high-level of professionals such as CEO to CTO of an organisation [79]. The phishers usually craft their messages so that they have various range of tones such as greed, urgency, curiosity, helpfulness, fear with the goal to lure the target persons into taking the baits.

This study therefore examined the phishing susceptibility level among healthcare staff in Ghana amidst work and perception factors. It seeks to determine the effect of work factors and perception of healthcare staff and their phishing appraisal threat levels and the ability to resist phishing bait. Such knowledge would help hospital authorities to adopt better strategies to improve upon the security practices of the healthcare staff in a way towards mitigating real attacks. This is a combined study which the targets' actual phishing susceptibility behaviour is assessed together with their self-reported security practice relating to a phishing. To achieve a better phishing simulation study, a comprehensive literature review on phishing simulation attacks was first conducted to assess and analyse already used techniques or methods, tools and to determine gaps in the existing studies. Additionally, ICT, as well as cyber security practices, were observed in the hospital. This provided better knowledge for the researchers to launch a simulated SMS-based phishing attack termed as smishing [49, 86]. This study contributes to the body of knowledge in various ways. The relationship between the actual and self-reported phishing behaviour of the healthcare staff were assessed. Furthermore, our study examined the relationship between work factors and psychological factors on self-reported behaviour relating to phishing. The psychological constructs which met the needs of the study objective were drawn from the health belief model (HBM) [58, 55] and protection motivation theory (PMT). The the state of the arts pertaining to phishing simulated study in healthcare was provided. Ethical aspects of in-the-wild study were also assessed. Furthermore, the reasons why the healthcare staff fell victim to the attack were also collected and examined. To the best of our knowledge, this is the first of its kind within the healthcare space that we conducted such an intensive study, guided by the state-of-the-arts studies. The paper is structured as follows; the background of psychological and work factors in phishing simulation study is presented. This is followed by the study approaches. The findings on the state of the art, click rates and the survey are then shared. The results are subsequently discussed and the conclusion is presented.

10.1.1 Perception and work factors with phishing simulation study

Falling victim to a phishing attack is more dominant in security attacks because attackers tend to exploit the psychological factors of their target persons into clicking the links [15]. However various studies [1, 29, 30, 67, 78] in phishing susceptibility in healthcare have not explored these psychological theories except a study by Jalali et al. that explored theory of planned behaviour and collected felt trust [41]. This gap in the literature provides basis for our study in which we explore the relationship between work factors and psychological factors that can be influenced to improve in security behaviour relating to phishing attack. This study therefore explores perception constructs in HBM and PMT. Perception relates to the mindset and psycho-socio-cultural effects of users' of an IT infrastructure and how that affects cyber security practice. HBM and PMT theories have extensively been used to explain human behaviour and have been found useful in assessing other information security practices among users [6, 35, 55]. For instance, Ng et al investigated into computer behaviour of users having used the HBM. They study identified perceived susceptibility, benefits, and self-efficacy to be determinants of email related security behavior [55]. Anwar et al. showed that gender has effect in security self-efficacy. Moreover, Humaidi et al proposed a comprehensive framework for analysing security practice based on various perception theories [35]. Infect a mapping review on related theories that have been used in assessing security practice was conducted by [92] and identified various perception constructs including perceived vulnerability, and perceived barriers. Much as these studies showed that perception constructs are widely used for assessing the motivation in information security research, the specific context (i.e. phishing in healthcare) can have major influence on the behavioral intention of users [41]. For instance, the perception of the severity of impact of a non-critical infrastructure may be lower than that of a critical infrastructure such as healthcare in data breach scenarios that violate the availability trait.

In assessing security practices related to phishing among healthcare staff, we therefore opine that it is necessary to explore perception factors in relation to phishing susceptibility. Such factors can then be improved for better security practice in phishing through various intrinsic and extrinsic motivations [18, 19]. To this end, psychological constructs that were used in HBM and PMT were deemed suitable to achieving this study objective.

In HBM, the predictor of a person's possible health related behaviour is dependent on the believe of the health threats (illness disease) and the effectiveness of the recommended actions(treatments and medicines) [16, 55, 55]. Back in the 1950s, this was derived to prevent sicknesses or help already sick persons to recover. HBM has been widely used in the healthcare sector as people can perceive the severity of disease and the recommended action

to make better health behaviour choices. HBM has found its way into observing information security practice in the human aspect of information security [92, 36]. For instance, the human aspects are normally observed for their security susceptibility perception and their belief in the organization's cyber security policy to predict their likelihood behaviour [55]. HBM consists of perceived susceptibility or vulnerability (PV), perceived severity (PS), perceived benefit(PBf), perceived barriers (PB), cues to action (CA), and self-efficacy (SE). PV is the risk perception of contracting a disease or falling victim to a cyber attack while PS is the perception of the adverse impact of the respective disease (death, disability, family life, or social relation) or security attack (loss of data, punishment, etc). PB is viewed as obstacles that are to be overcome in order to follow recommended solutions. In the same trend, the assessment of one's ability or confidence level to follow the recommended solutions is known as perceived SE. Additionally, CA is internal or external stimuli that influences one to adapt to the recommended solution. Stimuli include pain, disorders, advice, and knowledge of the situation of victims. PBf includes the perception of the available opportunities of the recommended course of actions. Common drawbacks that have been opined include its limitation to measure attitude, habitual behaviour, environmental or economic factors with the assumption that the threat knowledge is known by all persons.

PMT on the other hand consists of threat and coping appraisals which are used in decision-making by persons under stressful or harmful circumstances [52, 37, 95]. The decisions usually aim towards protecting oneself. The threat appraisal consists of PV and PS which the person who is involved in the stress or harmful situation, uses to appraise the level of the threat. PV measures the level of susceptibility of the person while PS is used to gauge the level of severity of the threatening event. Furthermore, the coping appraisal consists of response-efficacy (RE), SE, and response cost (RC). Within the context of PMT, RE is the perception of the effectiveness of the recommended action while RC is the cost component of the recommended measures.

10.1.2 Work factors and security practice

In addition to the psychological factors, the work of healthcare staff is characterised by erratic workload [95, 41, 5] and work emergency [92, 94].Work factors in this study refer to work related events, such as workload and work emergency that are associated with the use of IT systems in healthcare. Workload consists of the quantum of tasks that one has to perform within a given period, while work emergency refers to the urgency involve to accomplish a given task [21]. Particularly in healthcare, time is an important factor where therapeutic measures can be required in a timely manner without which lives can be lost. In some situations, patients can queue for

many hours waiting to be seen by scarce healthcare professionals. All these create work related stresses which can have an impact on the phishing related behaviour of the healthcare worker. Even though various research activities [35, 6, 36, 73] dealt with the perception aspect of security practice in healthcare, but little is known about how work factors (workload, work emergency) contribute to cyber security practice among healthcare workers. Jalili et al made effort to address that by analysing how workload contribute to cyber security behaviour in phishing [41]. However, work factors in healthcare was not completely addressed as work emergency was not included in the study. Besides, workload that was included, only served as a moderating variable and was not related with the perception variables to assess the effects. That is why we ague that since workload and work emergency are mostly associated with healthcare especially in COVID-19 pandemic, security practice ocan be impacted either directly or indirectly. This gap was also realised and proposals for empirical studies [96, 92, 94]. Relying on the aforementioned thoughts, the following research questions and hypotheses were formed:

- RQ1:What is the state of the arts in phishing simulation studies in healthcare?
- RQ2:How can phishing attack simulation study be conducted successfully in healthcare without interfering with the hospital's normal operations and exposing their system to potential attacks?
- RQ3:Are healthcare workers susceptible to phishing attacks?
- RQ4:What circumstances trigger healthcare workers to click on malicious link?
- RQ5:What is the relationship between the actual behaviour and self-reported behaviour among healthcare workers?
- RQ6:What is the ethical requirements for an in-the-wild-field study in phishing simulation?

In a similar study, Jalili et al estimated the effect of self-reported behaviour on the actual behaviour related to phishing attack [41]. In that vain we tried to compare the self-reported security behaviour related to phishing and the actual behaviour of healthcare staff of having clicked the link. As this study focus on assessing threats of phishing attack among healthcare staff and their ability to counteract, we expect that staff of hospitals have a good perception of security practices. Meaning that the healthcare staff can appraise security threats, overcome risky perceptions to comply with the security policy amidst work factors and perceptions as shown in figure 10.1. Based on this objective, we hypothesized that:

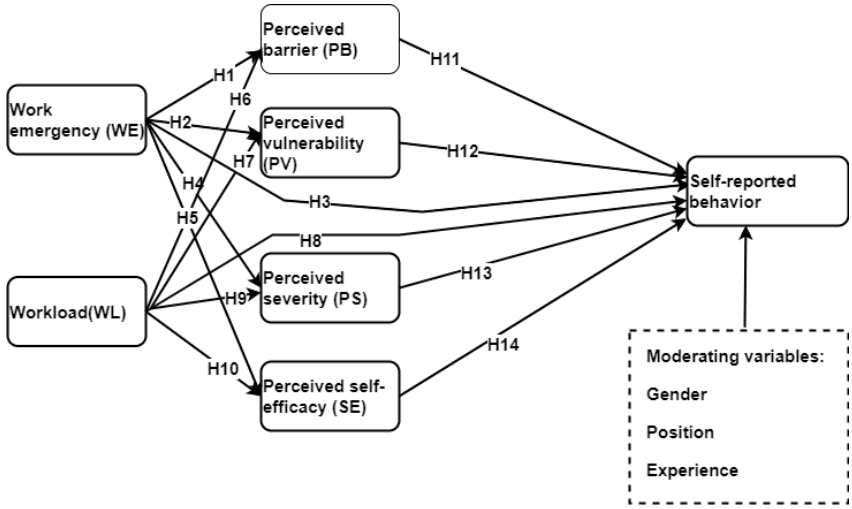


Figure 10.1: Research model for SMS-based phishing simulation study

- H1: Work emergency has negative influence on perceived barrier .
- H2: Work emergency negatively influence perceived vulnerability .
- H3: Work emergency has a negative influence on self-reported security behaviour (IB).
- H4: Work emergency is negatively related to perceived severity risk.
- H5: Work emergency has a negative effect on perceived self-efficacy .
- H6: Workload has adverse influence on perceived barrier.
- H7: Workload is negatively related to perceived vulnerability.
- H8: Workload has a negative effect on self-reported security behaviour.
- H9: Workload has negative influence on perceived severity.
- H10: Workload has a negative influence on perceived self-efficacy.
- H11: Perceived barrier has a negative influence on self-reported security behaviour.
- H12: Perceived vulnerability has positive influence on self-reported security behaviour.
- H13: Perceived severity has a positive influence on self-reported security behaviour.

- H14: Perceived self-efficacy has positive influence on self-reported security behaviour.
- H15: Perceived barrier has a negative mediating effect between work emergency and self-reported security behaviour.
- H16: Perceived barrier has a negative mediating effect between workload and self-reported security behaviour.
- H17: Perceived vulnerability has a positive mediating effect between work emergency and self-reported security behaviour.
- H18: Perceived severity has positive mediating effect between workload and self-reported security behaviour.
- H19: Perceived self-efficacy has a positive mediating effect between work emergency and self-reported security behaviour.
- H20: Perceived self-efficacy has a positive mediating effect between workload and self-reported security behaviour.
- H21: Perceived vulnerability has a positive mediating effect between workload and self-reported security behaviour.
- H22: Perceived severity has a positive mediating effect between work emergency and self-reported security behaviour.
- H23, H24 and H25 are respectively moderating variables of experience, gender and position that have potential effect on self-reported behaviour.

As shown in Figure 10.1, the latent variables of security perceptions including PV, PS,PB, SE, work emergency and workload are related with the intended security behaviour construct. Additionally, the model also showed the mediating effect of the perception factors between the work factor constructs and the IB. Position, work experience and gender were considered as the moderating variables.

10.2 Research methodology

Four approaches have been used in this study as shown in Figure 10.2.

First, a scoping review was conducted that aim at identify phishing simulating study methods/techniques, tools, and study gaps in practically assessed literature. Grey literature was also searched for phishing simulation tools.

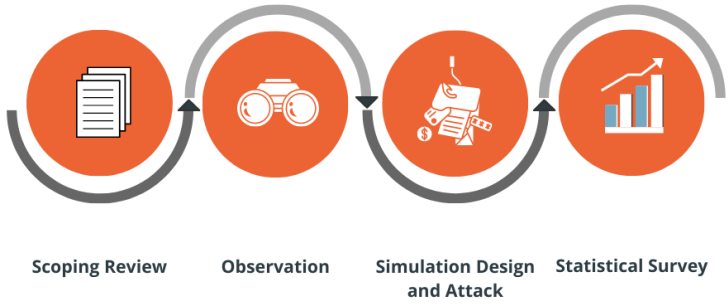


Figure 10.2: Study processes

This was followed by observing hospitals to understand the ICT and security practices in the hospital. Guided by these, an SMS-based phishing simulation study was set up and deployed. The deployment was done alongside a survey of both qualitative and quantitative approaches. Details of each approach are provided in the following subsections.

10.2.1 Scoping review

The aim of the review was to address the state of the arts by identifying, assessing, and analyzing the various approaches and techniques for use in critical infrastructure such as healthcare. A scoping review was adopted as the study aimed to assess, analyse and evaluate topics relating to phishing simulation in healthcare as categorised in table 10.1. We therefore searched for phishing related practical studies in healthcare in Pubmed, Google Scholar, Science Direct/Elsevier, IEEE Explore, and ACM Digital. The scoping review took place between September 2021 and December 2021. The following keywords and phrases, 'phishing attack', 'social engineering', 'healthcare', 'Information security practice' and 'information security behavior' .Boolean functions of 'AND', 'OR', and 'NOT' were used to combine the keywords. Peer-reviewed journals and articles were considered. Articles were first selected through a quick read-through of the titles, abstracts, and keywords for records that seem to match the inclusion and exclusion criteria. Duplicates were removed and the rest of the articles were fully read and assessed. Additionally, phishing related tools were further explored in grey literature with the key phrase "phishing tools" in the Google search engine. The findings were reported by adapting to Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) flow diagram10.5.

10.2.1.1 Inclusion and exclusion criteria

Only articles that were practically implemented in phishing related studies in healthcare were included in the study. Articles outside the scope including literature in other languages, except English, were excluded.

10.2.1.2 Data collection, categorization and analysis

In line with the objectives of this study, data collection and categorization were developed based on authors' discussions. The categories were defined purposely to assess, analyze, and evaluate the studies as shown in table 10.1. The identified articles were processed based on the categorise that were defined in table 10.1. A number of counts (n) and proportions were computed on each category.

10.2.2 Observation at the hospitals

We adopted a 'fly-on-the-wall-approach' by observing unnoticed of the healthcare workers' security practice. So the researchers were introduced to the healthcare workers as temporal staff of the IT department who were to collect feedback on issues relating to the information systems that were being used by the healthcare staff. We presume that healthcare workers would not behave in their usual way if they were aware that their security practices were being observed [74]. We observed general security practice but much attention was paid to physical security, internet use, email use, social media use, password management, incident reporting, information handling, and mobile computing as these areas are prone to security policy violations within the context of the human element [64, 63, 95, 89]. The purpose of this observation was to complement the review approach to answer RQ2 thus to understand effective methods of safely and effectively conducting phishing simulation study in healthcare.

10.2.3 Phishing simulation design and attack

With regard to social engineering tests, the goal was to determine if healthcare workers using IT systems are able to identify phishing related malicious messages amidst work factors and their perception. This approach was to find answers to RQ3 and RQ4 together with the hypotheses. Guided by findings from the observations, SMS based phishing was adopted in this simulation attack because the hospitals had not configured corporate email systems but rather uses mobile devices such as laptops and mobile phones in their provision for healthcare services. Since this was a simulated study, we did not want to use a critical infrastructure such as healthcare as a test range. Instead, these tests were conducted through the mobile contacts of

Table 10.1: Data categorization and definitions

No	Categorisation	Definitions
1	Methods/Technique	The scientific approach which was used in the study e.g. (a survey, simulated attack, interview)
2	Tools	Social engineering tools which were used in the study (e.g., gophish,)
3	Psychological, social and demographic (PSC) factors	Social engineering theories used to coerce targets into clicking on malicious links (PMT, TPB, TTAT)
4	Storyline strategy	Context within which adversaries craft phishing messages to bait targets
5	Cue	This defines the clue used in the study
6	Security and privacy measure of tools	This describes the behaviour of the tools (e.g., whether the tool collects some sensitive data of the target hospital and targeted persons in the study)
7	Ethical measures	This defines the consideration of the relative effect on participants (e.g. whether participants consented to the study)
8	Risk measures and measures to be adopted to conduct risk free assessment in the target environment.	
9	Social demographic factors	Factors such as gender, workload, emergency situations which were considered in the attack
10	Situational context of healthcare staff prior to clicking the link	This defines what the healthcare workers were immediately engaged in prior to clicking the link
11	Susceptibility reasons	This defines the reasons for clicking the link by the staff
12	Survivors bias	Analysis of the characteristics of healthcare workers who only clicked the link without considering those who did not click the link.

the healthcare staff. We opined that if healthcare staff can be security conscious on their cellphones, that could be translated into the healthcare environment. So the plan was that healthcare staff will receive a ”malicious message” with a ”malicious link”. If the target person clicks on the link, the click event would be registered in a database and the person would be redirected to a questionnaire instrument. While other studies have used multiple clicks in similar studies [79, 29], the goal of those studies are mainly to access the effectiveness of phishing related training and education. In this study, a click of the link was used, just as in a recent study conducted by [41]. This is because the goal of Jalali et al. and this current studies are geared towards assessing the effects of theoretical factors.

The questionnaire instrument was to support in identifying current circumstances that lead to the clicking of the link together with the behavioural intentions of that user. A secured domain name was registered to look similar to the hospitals' domain except that the domain name type was different (ie .info instead). This was the major phishing cue or clue that the researchers wanted to observe from the target. So a secured online questionnaire tool, Nettskjema [57], was used to design a questionnaire for this test. Nettskjema is deemed secured and privacy safe for developing questionnaires as compared to other online forms. Additionally, a website was developed with a database to collect the click events of users. To comply with privacy and security regulations, each click event was encrypted with SHA-256. The click events were collected alongside their date and time stamp in order to know when each click event occurred. The website was hosted with the registered domain and the link together with the phishing message was sent to the targets via SMS. The phishing message was chosen to reflect events that were ongoing at the hospital and the it was COVID-19 related as shown in figure 10.3. The simulation attack began on the 24th November 2021 and ended on the 8th of December 2021. After a week, we closed all responses to the questionnaire and made phone calls to participants to collect qualitative data relating to why they clicked the phishing link. Only participants who remembered having received the SMS and read the content were given audience to provide their responses.

If a respondent clicks on the link of the questionnaire, the click event first is registered in the database and then opens the questionnaire. To understand the security practice of the respondents, to collect information from the respondents concerning what he or she was engaged in just before clicking the link. The purpose of collecting the information was to understand why the user clicked on the link. For example, the respondent was busy serving patients, etc. This will provide input into providing the needed training in regards to phishing attacks. The Personally identifiable records of respondents were not to be stored in the database, and of course, the link was not actually malicious as depicted in figure 10.4.

Hello,
Your name came up during contact tracing of a victim diagnosed with the delta variant of the coronavirus.
Kindly click the link www.[redacted]
[redacted].info for more detailed information and complete the form to enable the team reach out and assist you with treatment.
Kindly remember to keep this information confidential and private and talk to the team if you have any queries.
Regards, [redacted] Covid-19 Management Team

Figure 10.3: Deceptive message for SMS-based phishing simulation

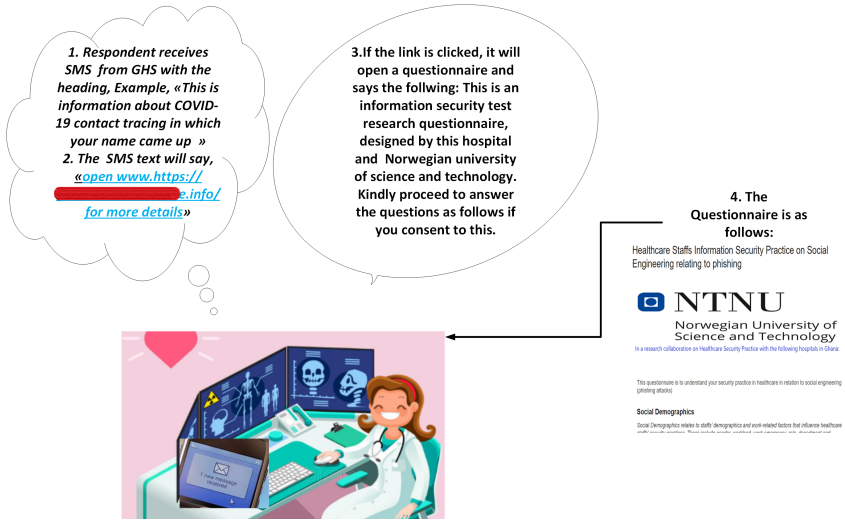


Figure 10.4: Framework for SMS-based phishing simulation

10.2.4 Statistical survey

A total of 167 healthcare staff agreed to join the study through a convenience sampling. Due to ethical, privacy, and security concerns, the identity of these hospitals and the respondents have not been disclosed in this paper. To deal with survival biases [41, 11], participants who did not click the link and those who clicked the link but failed to fill out the questionnaire were contacted by phone to find out their reason for doing so.

The questionnaire instrument in this study has a social demographic section that collected attributes such as gender, position at work, and length of years of experience of the respondents. Another section collected data on the work situation such as the workload, work emergency, what the participant was engaged in and his or her expectation prior to clicking the link. Security practice items relating to perceived barrier, perceived vulnerability, perceived severity and perceived self-efficacy were also included in the study as shown in table 10.9. A Likert scale of 5 options was used. The questionnaire were crafted to cover security practice relating to internet use, email use, password management and social media use. These aspects of security practice are mostly prone to security violations by the human element [92, 96, 64]. These questionnaire items were adapted from existing questionnaire and modified for this study as shown in table 10.9 in appendix 10.6.

10.2.5 Ethical, privacy and security measures

When participants realise their behaviour is monitored, they tend to behave differently. On the other hand, when they are monitored without consent, researchers are accused of breaking laws [7, 74]. Deceptive means, researchers have intentionally refused to disclose some of the research procedures and purpose in order to have an unbiased study [74]. Meanwhile, studies involving deceptiveness are proven to be effective because they assess the real responses to phishing, the potential threat attacks that are yet to occur, and can effectively measure the success rate of countermeasures that are yet to be deployed [74, 7].

Many ethical committees fail to approve phishing related studies because they believe that deception in research contradicts informed consent and is potentially harmful to participants, invading privacy, breaking participants' rights, and limiting their control of risks (such as stress or psychological damage) associated with the research. However, the research community opposed this view. Various studies have stated that deception in research is not ethically wrong and the reason for withholding such information is what the ethical committee should be assessing instead [7, 77]. They also explained that people in the clinical sector enjoy deception in research if it is likely to educate them. The participants were even interested to participate again in similar deceptive researches [74, 7].

Psychological association supported the debate and said it may be impossible to study some psychological constructs without withholding certain information about the true purpose of the study or deliberately misleading the participants [74]. British Psychology Society also agrees to deception in research and said that the awareness of participants about some aspects of the study could likely compromise its validity [74, 7].

In essence, it is justified to use deception as a research method to have valid inference if it has a kind of road map The road map is as follows:

- Pre-launch of phishing: prepare fraudulent text, issue press release to administrators, and pre-inform consent
- Launching the attack: consider data protection, consider the well-being of the participants
- Post launch: consider debriefing, post informed consent and data protection

Having followed these measures, the participants volunteered and consented to the study and also shared their phone numbers for this research. The healthcare facilities that joined this study, adopted full electronic health record systems in their operations and elected to join the study through an invitation. Ethical clearance was obtained in Ghana. Following that, research coordinators were appointed to liaise with the management of these hospitals to facilitate the study. For instance, the facilitators identified SMS platforms and sent the phishing SMS messages together with the phishing links to the targets. Because of the high cost of internet data bundles in Ghana, the target participants who filled the questionnaire after clicking SMS received a reimbursement of their internet data amounting to GHS 10.00 each (which is about USD1.67). Prior to filling out the form, participants were debriefed and reminded of their earlier consent to take part in the study. In addition, they were still given the opportunity to opt out if they changed their mind.

10.3 Findings in this study

This section presents findings from the literature study, observation, simulated phishing attacks, and the statistical survey results.

10.3.1 Scoping review findings

As presented in Figure 10.5, 60 papers were initially identified from scientific databases of which 2 were duplicates. Additionally, 16 sources of tools for phishing simulation studies were identified. Through readings, 23 records were excluded remaining 51 records which were eligible for a full reading.

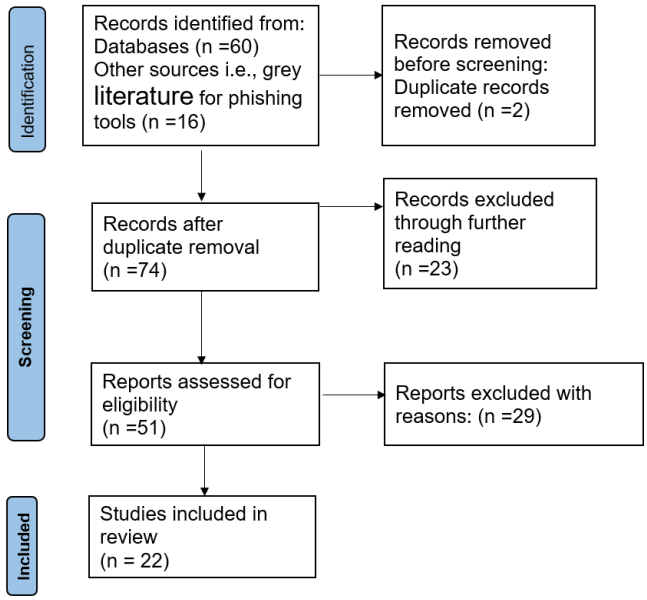


Figure 10.5: Report of literature: PRISMA diagram[68]

In the end, 29 records were further removed because these papers were not specifically in the healthcare domain(eg [47, 70, 45, 25]), not precisely within the scope of phishing simulation (eg [59, 14]). These were not clear in the identification stage until the full assessment stage.

In the end, 22 studies (as shown in figure 10.5) comprising of 6 scientific articles (shown in Table 10.1) and 16 grey literature sources (shown in table 10.3) were included in the study. From the 6 articles, one study used only survey, four studies used only in-the-wild field study with an email-based phishing attack and one of them combined both email-based method and literature survey [41].

Additionally, three groups (third party companies, custom-developed software tools, and commercial tools) emerged in the usage of a total count of five in-the-wild field phishing simulation tools. Gordon et al [30] used commercial cloud-based phishing simulation tools (representing 20%) but [78, 29] used custom developed tools while [41] and [67] used third party companies (each representing 40%) to conduct their phishing attack simulated studies. Out of a total of five simulated types of payloads that were used in the study, 4 (80%) of them simulated malicious link while 1 (20%) study [67] simulated credential harvest. The storylines that were used include health concerns [1], disposition to trust and risk-taking tendency, [67],

Table 10.2: Literature review categorization results.

Article	Method	Tool	payload	Story line	Attack Types
[41]	1.In-the-wild field study, 2. survey	Third party company	simulated malicious link		email
[1]	survey			Health, concerns, disposition to trust, and risk-taking propensity	
[29]	In-the-wild field study	custom-developed software tools.	simulated malicious link		email
[30]	In-the-wild field study	Cofense formerly PhishMe (commercial)	simulated malicious link		email
[67]	in-the-wild field study	Third-party company	credential harvesting, batch files obfuscated	marketing, advertising potential employment positions	email
[78]	in-the-wild field study	custom developed software tools	simulated malicious link	IT support request	email

marketing, advertising potential employment position, and [78] offer of IT support services. Amidst various attack types such as email-based, voice-based and SMS-based, all the studies (except [1] that did not indicate the attack type) used email-based as shown in table 10.1. Slonka et al further indicated the phishing cue in the domain name type avoided the storage of clients' passwords, and used SSL to secure the interactions with clients [78] as measures towards enhancing ethics, privacy, security, and risk measures. Jalali et al also submitted a questionnaire to those who click the link and those who did not click the link in a way to observe survival bias. In addition, the investigators did not collect contact information of the healthcare staff in an effort towards observing security and privacy measures [41].

Furthermore, out of the 16 phishing simulation tools (see in table 10.3) that were identified, 7(43.7%) were open source while the remaining 9 (56.3%) are commercial tools. Additionally, 6 (37.5%) could be deployed on the company network premise (premise-based) but the rest 10 (62.5 %) were cloud-based and inherited the cloud-related risks.

10.3.2 Observation study

In terms of how to launch a simulated attack in the hospital, it was realised that the hospitals did not configure corporate email addresses and their network was limited to local area network (LAN). Their healthcare staff could only access the EHR systems within the hospital premises without an internet connections. The hospital's network had an internet connection to enable access to APIs and also to enable remote desktop access to the EHR. Additionally, the healthcare staff were using mobile devices such as laptops

Table 10.3: Phishing simulation tools.

No	Tool Name	Type	Cloud/On-Premise
1	GoPhish [27]	OpenSource	On-premise
2	Phishing Frenzy[66]	Open-source	On-premise
3	King Phisher[65]	Open-Source	On-premise
4	Simple Phishing Toolkit (sptoolkit)[82]	Open-source On-premise	
5	Social-Engineer Toolkit (SET) [85]	Open-source	On-premise
6	SpeedPhish Framework (SPF) [81]	Open-source	On-premise
7	SpearPhisher BETA [42]	Open-source	
8	Barracuda Phishline [12]	Commercial	Cloud
9	Cofense [22]	Commercial	Cloud
10	Hoxhunt [34]	Commercial	Cloud
11	InfoSec [39]	Commercial	Cloud
12	IronScales [40]	Commercial	Cloud
13	Lucy [46]	Commercial	Both
14	Mimecast [48]		
15	KnowBe4 [43]	Commercial	Cloud
16	Proofpoint [69]	Commercial	Cloud

and mobile phones in deliver healthcare services. Observational findings in other areas such as physical security, password management, incident reporting, and information handling are less relevant to this phishing study and have not been reported in this paper.

10.3.3 Phishing clicks

Out of a total of 167 healthcare staff who were targeted in the SMS-based phishing simulation study, 102 (61.1%) clicked the simulated malicious link but 65 (38.9%) healthcare staff were not susceptible to the attack. Furthermore, 25 (24.5%) participants out of the 102 who clicked the link, answered the questionnaire whose link was embedded in the study. So a total of 77(75.5%) failed to answer the questionnaire. The clicking behaviour was

high in the start of the simulation attack but sharply decreased after the first 2 days as shown in the graph on Figure 10.6. Additionally, the intended phishing security behaviours were generally lower (as shown in Figure 10.9) than their actual behaviour across all the roles of the healthcare staff who participated in the study.

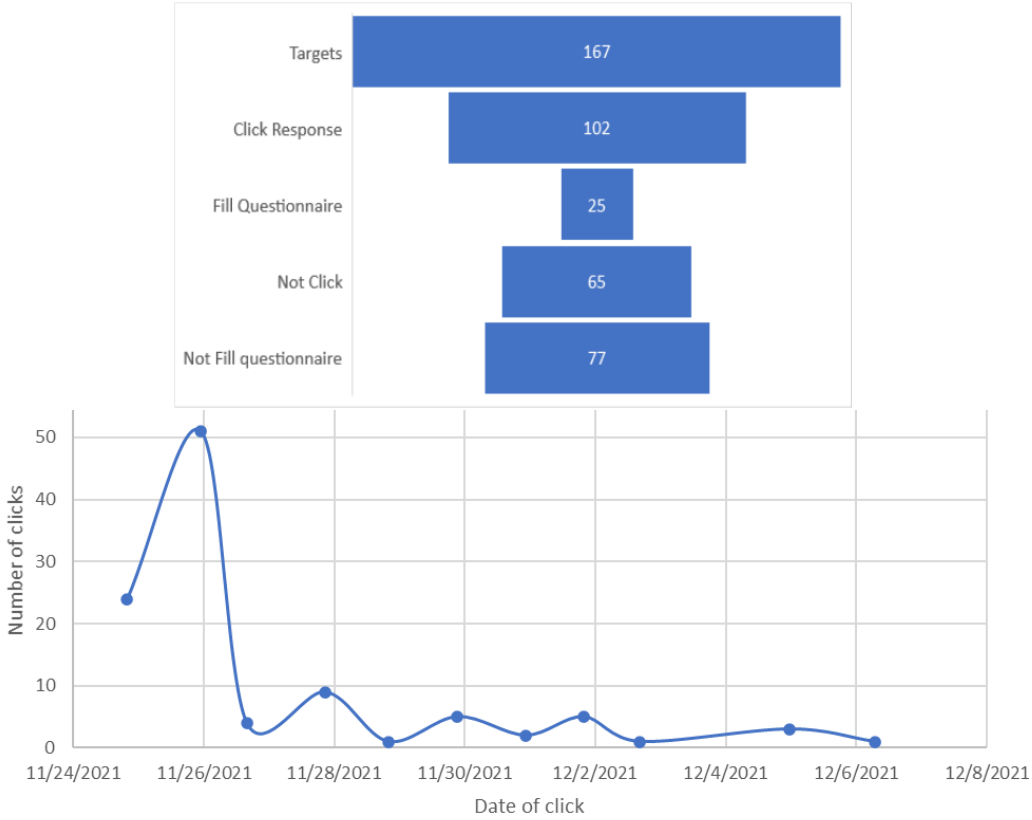


Figure 10.6: Phishing click statistics

10.4 Statistical analyses

The population profile of participants who clicked the link and answered the questionnaire is shown in table 10.4. The proportion of males (44%) and females (56%) was similar but the age range between 30 and 40 was the highest (72%). Nurses constituted the majority of the participants' population by 52%. None of the participants had less than one year of work

Table 10.4: Descriptive statistics of healthcare staff who clicked on the simulated malicious link and answered the questionnaire.

Category	Value	Freq.	%
Gender	Male	11	44.0
	Female	14	56.0
Age range	20-29	6	24.0
	30-39	18	72.0
	50-59	1	4.0
Position	Pharmacists	2	8.0
	Doctor	2	8.0
	Nurse	13	52.0
	IT personnel	1	4.
	Lab personnel	1	4.
	Data Manager	1	4.0
	Public health	4	16.0
	Others	1	4.0
Work experience	less than 1 Year	2	8.0
	1-5 Years	11	44.0
	6-10 Years	6	24.0
	11-15 Years	5	20.0
	21-25 Years	1	4.0
	Total	25	100.0
Click location	Off duty	14	56.0
	On duty	11	44.0
	Total	25	100.0
Engaged in	Not disclosed	10	40.0
	Patient care	8	32.0
	Admin duties	2	8.0
	Leisure	3	12.0
	House chores	2	8.0
Expectation	Believed in the subject of the message	17	68.0
	Was curious	6	24.0
	Not Disclosed	2	8.0

experience. An almost equal proportion of the participants were off duty (56%) and on-duty (44%) with 32% engaged in patient care and administrative duties (%8) while the reaming (40%) failed to disclose what they were engaged in. A total of 17 (68%) out of the 25 participants believed in the subject of the phishing message, 6 (24%) were curious and only 2 (8%) did not disclose their expectations prior to clicking the link.

10.4.1 Reliability, validity, fit, structural model and correlation

The reliability of the constructs was assessed with Cronbach's alpha(CA) and Composite Reliability (CR) as shown in Table 10.5. All the CR values of the constructs were greater than 0.700. Additionally, the values of all the constructs of the average variance extracted (AVE) were greater than 0.500 which thereby met the convergence validity. The results for validity are also presented in Table 10.5. Discriminate validity was assessed with Fornell-Larcker, Heterotrait-Monotrait Ratio (HTMT), and cross factor loading of all the items. Having assessed the entire model, the values of R^2 were computed to be 0.369, 0.116,0.086, 0.293 and 0.554 for perceived barrier, perceived severity, perceived vulnerability, self-efficacy and Self-reported behaviour variables respectively while the Q^2 were obtained to be 0.312, 0.036, 0.003, 0.229 and 0.405 for the respective variables.

Table 10.5: Reliability and validity assessment

Construct	Reliability and validity				Discriminate analysis: Heterotrait-Monotrait Ratio (HTMT)						
	CA	rho_A	CR	Average Variance Extracted (AVE)	IB	PB	PS	PV	SE	WE	WL
IB	0.835	0.934	0.886	0.664							
PB	0.799	0.826	0.881	0.714	0.578						
PS	0.746	1.043	0.839	0.638	0.400	0.666					
PV	0.772	0.921	0.892	0.805	0.248	0.444	0.652				
SE	0.701	0.703	0.834	0.626	0.596	0.613	0.434	0.494			
WE	0.667	0.675	0.857	0.750	0.364	0.715	0.415	0.163	0.277		
WL	0.429	0.572	0.758	0.619	0.789	0.730	0.071	0.367	0.765	0.371	

The model was then used to further test our hypothesis to determine the significance of the relationship. As shown in Figure 10.7, and Table 10.6 all hypotheses from H1 to H14 were evaluate to determine if PV, PS, PB, SE, WE, WL, and all mediating effect (from H15 to H22) have a significant effect on self-reported cyber security behaviour (IB) related to phishing among healthcare workers. Additionally, the model was used to assess the effect of gender, position and work experience as moderating variable as shown in Figure 10.7, and Table 10.6. The findings shown in Figure 10.7, and Table 10.6 revealed that work emergency had a significant negative effect on perceived barrier risk as defined in the first hypothesis (H1) with the value of -0.46 at p-value=0.00. Additionally, workload has a significant positive effect on perceived self-efficacy as defined in H10 with the value of 0.50 at p-value=0.02. Aside, none of the constructs (PV, PS, PB, and SE) has a significant effect on IB risk. Moderating variables of gender, position, and years of work experience also showed no significant impact on IB.

Furthermore, as shown in table 10.7 Pearson's correlation of the valid constructs showed that perceived barrier (PB) was positively correlated with

Table 10.6: Structural Model

Path	Hypothesis	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	P Values
Work emergency ->Perceived barrier	H1	-0.46	-0.48	0.14	**0.00**
Work emergency ->Perceived vulnerability	H2	0.13	0.12	0.25	0.60
Work emergency ->Self-reported behaviour	H3	0.18	0.15	0.26	0.49
Work emergency ->Perceived severity	H4	0.35	0.35	0.26	0.18
Work emergency ->Self efficacy	H5	0.13	0.09	0.24	0.60
Workload ->Perceived barrier	H6	-0.31	-0.32	0.19	0.10
Workload ->Perceived vulnerability	H7	-0.27	-0.20	0.30	0.38
Workload ->Self-reported behaviour	H8	-0.13	-0.17	0.30	0.66
Workload ->Perceived severity	H9	-0.03	-0.03	0.28	0.91
Workload ->Self efficacy	H10	0.50	0.52	0.21	**0.02**
Perceived barrier ->Self-reported behaviour	H11	0.31	0.27	0.32	0.32
Perceived vulnerability ->Self-reported behaviour	H12	0.42	0.35	0.29	0.14
Perceived severity ->Self-reported behaviour	H13	-0.53	-0.45	0.34	0.12
Self efficacy ->Self-reported behaviour	H14	-0.34	-0.34	0.32	0.29
Indirect effect					
Work emergency ->Perceived barrier ->Self-reported behaviour	H15	-0.14	-0.13	0.16	0.37
Workload ->Perceived barrier ->Self-reported behaviour	H16	-0.10	-0.09	0.13	0.47
Work emergency ->Perceived vulnerability ->Self-reported behaviour	H17	0.05	0.05	0.12	0.66
Workload ->Perceived severity ->Self-reported behaviour	H18	0.02	0.04	0.17	0.92
Work emergency ->Self efficacy ->Self-reported behaviour	H19	-0.04	-0.03	0.11	0.71
Workload ->Self efficacy ->Self-reported behaviour	H20	-0.17	-0.19	0.21	0.41
Workload ->Perceived vulnerability ->Self-reported behaviour	H21	-0.11	-0.06	0.15	0.45
Work emergency ->Perceived severity ->Self-reported behaviour	H22	-0.18	-0.17	0.18	0.30
Experience ->Self-reported behaviour	H23	-0.06	-0.01	0.18	0.86
Gender ->Self-reported behaviour	H24	-0.31	-0.32	0.96	0.34
Position ->Self-reported behaviour	H25	-0.29	-0.26	0.32	0.38
	R^2	Q^2			
Perceived barrier	0.369	0.312			
Perceived severity	0.116	0.036			
Perceived vulnerability	0.086	0.003			
Self-efficacy	0.293	0.229			
Self-reported behaviour	0.554	0.405			

the self-reported behaviour intention (r=0.571,p-value=0.01). Additionally, workload (WL) was also realised to have a significant positive correlation with perceived self-efficacy (r=0.494, p-value =0.05). However, perceived self-efficacy (SE) risk negatively correlated with IB (r = -0.483, p-value = 0.05). Similarly, work emergency had a significant negative correlation with PB risk at (r = -0.401, p-value = 0.05).

10.4.1.1 Views of targets who did not click the link

In efforts to enrich this study, we had a phone conversation with participants who clicked the link but did not answer the questionnaire and those who did not even click the link. From figure 10.6, out of 167 healthcare workers who were targeted in the study, 142 failed to fill the questionnaire. Out of these, 28 provided feedback as to the reasons why they clicked the phishing simulation link without answering the questionnaire or why they did not even click the link. Eight of these respondents were males and the remaining 20 who provided the feedback were females as shown in figure 10.8.

The respondents who did not click the link said the message was malicious and some said they were busy and did not click the link. Some of those who did not click the link also claimed that the questionnaire items were many and others said they did not have time to fill out the question-

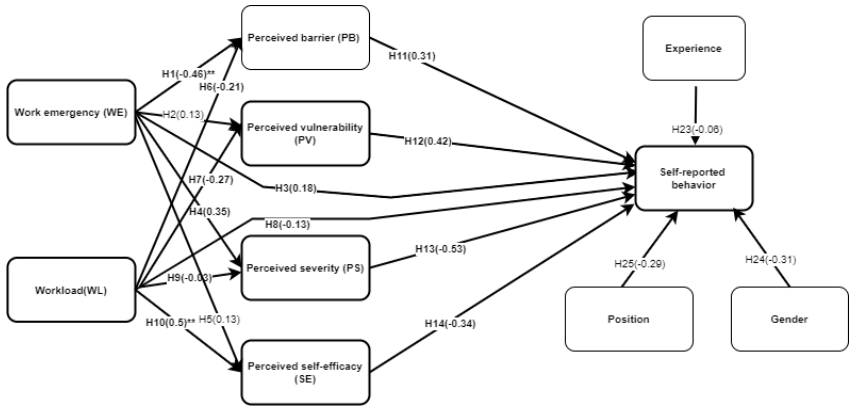


Figure 10.7: Research model with estimations

Table 10.7: Correlation between self-reported phishing behavior (IB)perception variables and work factors

	Correlations						
	WL	WE	PB	PS	SE	PV	IB
WL	–						
WE	.458*	–					
	0.021						
PB	-	**-**	–				
	0.334	**0.401***					
	0.102	0.047					
PS	0.023	0.208	-	–			
			.566**				
	0.912	0.319	0.003				
SE	**0.494***	0.241	-	0.038	–		
			0.441*				
	0.012	0.245	0.027	0.857			
PV	0.003	0.291	-.441*	0.450*	-		
					0.102		
	0.987	0.157	0.027	0.024	0.627		
IB	-	-	.571**	-	-	0.015	
	0.391	0.197		0.238	.483*		
	0.053	0.346	0.003	0.252	0.014	0.944	

**. Correlation is significant at the 0.01 level (2-tailed).

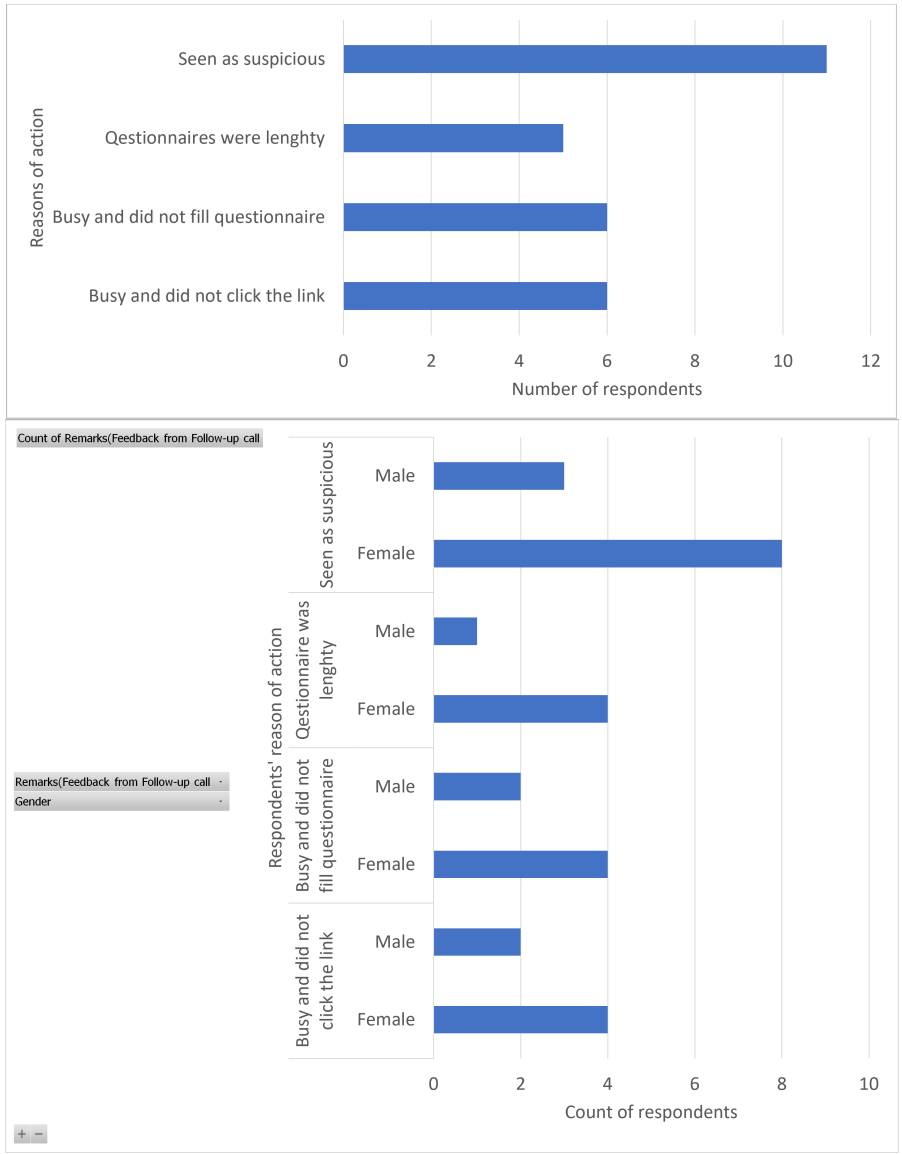


Figure 10.8: Feedback from respondents who fail to fill out the questionnaire and those who did not click on the link

naire. Eleven in total saw the message as suspicious and they comprised eight females and three males. Two males and four females, were busy and

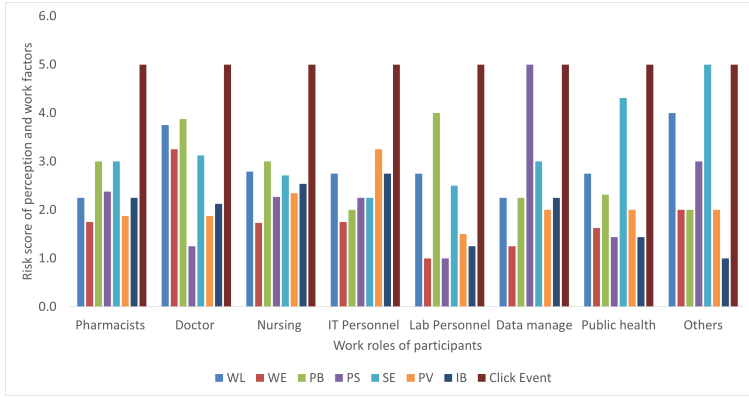


Figure 10.9: Comparing actual clicks with intended phishing behaviour of healthcare workers

did not click the link. Additionally, two males and four females claimed that the questionnaire items were many while four females and two males did not fill out the questionnaire because they were busy. The female proportion was generally high (71.5%) as compared to the males (28.5%). Similarly, the proportion of female were higher in all as compared to the males.

10.5 Discussion

The human aspect of cyber-security practice has become a major window in recent times for cyber-criminals to disturb healthcare organisations' operations through unauthorised accesses and data breaches [87]. In terms of ransomware, the human element is often baited through phishing attack to click on malicious links. The victims could therefore compromise healthcare cyber systems if they happen to be susceptible. They could end up installing remote connection tools, malware or even provide their user credentials to the attackers to enable them to move forward with their attack. Healthcare staff can fall victim to phishing attacks due to the nature of their work. They are often occupied with a heavy workload due to the high patients-to-healthcare staff ratio and their work is sometimes characterised by emergency situations, thereby, increasing their cognitive load [53]. Additionally, healthcare workers may have poor information security knowledge and training and poor perception which could lead them to undermine better cyber security hygiene in phishing attack [84]. Since most hospitals in Ghana are adopting EHR, many questions are being asked in the context of cyber security relating to a phishing attacks. To provide significant answers to these, a smishing simulation study backed by state of the art studies was

conducted among healthcare workers in Ghana and insight into the findings is discussed in the following sections.

10.5.1 Principal findings

The principal findings in this study are shown in table 10.8. In preparation for the implementation of this phishing simulation study, the hospital's environment was physically observed to gain an understanding of its IT systems and how the healthcare workers use these tools to provide healthcare. Before that, a systematic review was conducted to provide the state of the arts on various teams in phishing simulation attack context. The attack was subsequently launched together with a statistical survey. In the scoping review, six scientific papers were identified to have been practically assessed in phishing simulation studies in healthcare. A further search for phishing simulation tools in grey literature revealed 16 different types of phishing simulation tools. Email-based phishing attacks with in-the-wild studies and surveys were the two methods being used to conduct phishing simulated studies in healthcare. Out of this in-the-wild study, email-based was the commonest as shown in Table 10.2. Third-party companies, custom-developed tools, and commercial tools were being used in the state-of-the-arts of which third party companies and custom-developed software tools were often used. A simulated malicious link was often used as the payload and storylines including health concerns, marketing and advertising for potential jobs and IT support was used. Reconnaissance and intelligence gathering indicated that the hospital did not use corporate email system and most of the healthcare staff had not configured corporate emails. So the hospital was using mobile devices such as laptops and phones in communications and accessing EHR in their healthcare delivery.

From the 167 targeted healthcare staff whom the simulated phishing messages were sent, more than half (61.1%) fell victim to the attack but only 25 (24.5%) of the victims filled a questionnaire and indicated varying reasons for their susceptibility. For instance, 7 (68%) out of the 25 participants believed in the subject of the phishing message, 6 (24%) were curious. The CA of workload and work emergency were slightly lower with CA values of 0.667 and .429 respectively, however, their corresponding CR values were above 0.700. It has been noted that, if the number of questionnaire items measuring the construct is 10 or more, the coefficient of CA is expected to be 0.6 or higher [75, 31] otherwise, it is usual for the CA values to be around 0.5. Based on the view that just one click is needed in phishing susceptibility attack to achieve the adversary's goal, 167 participants resulting in the 61.1% susceptibility rate, meets the significant requirements. Other related phishing simulated studies have similar or lower participants [3, 28].

10.5.2 Work factors and perception risks in relation to self-reported phishing risk behaviour

In the report, all the factor loading values were greater than their corresponding cross-loading indicating valid discriminate validity [44]. Also, the HTMT values were below the limit of 0.9 indicating the discriminate validity of the constructs [44, 32]. Additionally, the variance inflation factor values were below the threshold of 5, indicating no issues of multicollinearity [32].

R^2 refers to the effect or changes in the dependent variable's influenced by the independent variables and this is expected to be equal to or greater than 0.10 in order for the related construct to be adequate for predictions [24]. Aside from perceived vulnerability (PV) which recorded an R^2 of 0.086 all the dependent constructs of PB, PS, SE and self-reported behaviour met the 0.10 threshold as shown in table 10.6. Though the R^2 of PV is slightly lower than 0.01, other sources [83, 33] indicate that such model can be used for explaining the relationship between variables either than prediction. Q^2 measures the predictive relevance of the model of which the value is expected to be greater than 0 in order for it to be relevant [4]. To this end, and model was generally fit and was used for the estimation as shown in Table 10.6 and Figure 10.7 using structural equation model (SEM) of SmartPLS [72]. SEM is known for the purpose of estimating causality among variables in the structures of various equations [13].

Assessing the contribution of work factors and perception variables with self-reported cyber security behaviour, the results showed that work emergency (WE) negatively predicted PB (r-0.46, p-value=0.00) and this supported H1. The remaining hypothesis were not significantly predicted with the SEM model . Furthermore, workload significantly predicted PS in the positive direction as opposed to our hypothesis H10 as shown in Table 10.6 and Figure 10.7. Additionally, a validation with Spearman's correlation showed that workload also significantly predicted self-efficacy risk (r= 0.494, p-value = 0.05) and work emergency predicted perceived barrier risk in the reverse direction at the significance of r= -0.401, p-value = 0.05. These predictions were similar with that of the SEM.

Additionally, workload (WL) was also observed to have a significant positive correlation with perceived self-efficacy (r = 0.494, p-value = 0.05). This is in contradiction with our initial assertion of H10. Meaning that, as the workload of the healthcare staff increases, they tend to perceive that they are unable to cope with additional responsibilities of security practice, they by, increasing their perceived self-ability risk of complying with security regulations. The healthcare staff could as a result be susceptible to phishing tricks. This also supports our initial assumption. A similar study by Jalali et al also found a causal effect of workload on the phishing risk behaviour of healthcare staff [41]. Similarly, work emergency had a significant negative effect with PB risk. This translates that higher work emergency among

healthcare staff corresponds to lower risks of PB. Consequently, a lower risk of PB is also a significant positive predictor of phishing susceptibility behaviour as shown in Table 10.7. This can possibly be related to findings in table 10.8, where a qualitative finding revealed that six of the healthcare staff were busy and did not click the link. Though not proven to be statistically significant, it could mean that, during an emergency, the healthcare workers tend to prioritise patient care and subsequently fail to be susceptible to a phishing attack. So further training and awareness could possibly be a boost to their effort of conscious care behaviour.

A further step of analysis with correlation showed that PB was positively correlated with IB at (r=0.571, p-value =0.05). This contradicts our hypothesis H11 we originally presumed that PB negatively correlates with IB. Perceived barriers are obstacles that can inhibit secure phishing related security behaviour. The results, therefore, suggest that higher perceptions of obstacles to secure phishing practices are related to an increase in self-reported conscious care phishing security behaviour. If the relationship was a causal effect, it would have been translated to mean that removing perceived barrier risks will improve phishing security-conscious care behaviour. Related studies in general cyber security behaviour and awareness [6, 55] did not show statistically significant results to support this or otherwise. Additionally SE risk negatively correlated with IB (r = -0.483, pvalue=0.05) as shown in Table 10.7 which translates that the perceived risk of the assessment of the healthcare workers' ability to comply with phishing security policy, decreases with corresponding increases of their phishing security risk behaviour. This contradicts the initial assertion (H14) as we expected SE to positively correlate with phishing related security behaviour. This could therefore mean that healthcare workers who think they have the ability to overcome phishing tricks do not in fact have and that is why they were susceptible to this attack in the first place.

However, all mediating and moderating variables were assessed and they did not have any significant effects on the study. This indicates that, the effect of those variables are statistically equal to zero. With regards to phishing simulating studies in the healthcare context, this is the first of which these specific variables were drawn from the HBM and PMT to design this model. A related study that used constructs from the theory of plan behaviour showed a positive prediction of attitude, subjective norm, and perceived behavioural control [41]. That study further indicated that workload was positively correlated with phishing-related practice. Relating to the study, the sample size in this work was relatively small, therefore, further studies with adequate sample size are required to arrive at a more valid conclusion.

10.5.3 Phishing attack methods, tools, risks measures, payload and storyline

From the state of the art, six scientific studies were published on phishing practical studies in the area of healthcare. Some of the studies [29, 30, 67, 78] used in-the-wild study approach, but [1] used questionnaire based survey while [41] combined both in-the-wild and the questionnaire survey. With these few studies, it is clear that there is a huge gap in the practical assessment of healthcare workers' phishing simulation studies. So little knowledge has been contributed so far in the scientific community towards understanding security practices in phishing security conduct among healthcare workers. This might have possibly contributed significantly to the knowledge gap of healthcare staff and resulted in the numerous successes in ransomware attacks in healthcare. The low account of phishing simulation study in healthcare might have been due to the critical nature of healthcare and the strict regulatory requirements needed to conduct such studies. Furthermore, according to Salah et al, phishing simulation study consists of three types which are self-reported survey, laboratory experiment and in-the-wild study [74]. Self-reported surveys are ineffective due to biases from participants and researchers. Laboratory controlled experiments are also known to be unreliable as they create an artificial environment for participants. An In-the-wild field study is considered reliable since participants are observed in their natural environment. The challenge associated with the in-the-wild study is ethical issues as it involves deception. Another issue is how to collect feedback from targeted participants in a phishing simulation study. To overcome these, recommended road maps for safely conducting the study and survey instruments with follow-up contacts can be used to have an effective study.

Email-based phishing is one of the preferred attack methods used by cybercriminals to launch phishing attacks [51, 17]. Malicious links are usually embedded in the emails and sent to the targets with messages enticing them to click the links. The links are usually associated with payloads such as malware installations, malicious attachments, harvesting of sensitive information such as credit card numbers, personal identification numbers (PINs), social security numbers, and other bank details. The email-based attacks are popular in this state of the art merely due to the widespread usage of email systems among organisations. Unfortunately, the healthcare systems that were involved in this study had not begun to use corporate email systems. But as phishing attacks include VOIP and SMS, instant messaging, and social networking sites, SMS-based phishing was therefore adapted in this study combined with a questionnaire-based survey. The combination of the SMS-based and the questionnaire were very essential in this work because the SMS helped to measure the susceptibility level (click/not click) of the healthcare staff while the questionnaire helped in measuring the percep-

tion and work factors that possibly contributed to the susceptibility. Clearly, each of these methods alone would not have been able to meet the study objective and as email system was not configured in the target hospital, it was basically not an option.

Regarding phishing simulation tools, third-party security companies, custom-developed tools, and a commercial tool were identified in the state-of-the-arts as shown in Table 10.2. Appraising privacy, security, and ethical concerns, this study did not use third-party companies since the scope of the ethical clearance did not include giving out contact information to third-party companies. So we developed custom software and hosted it with an SSL certificate to record the click events of the targets. The SMS were hence sent via an SMS messaging company however, to avoid privacy and security issues, the contact phone numbers of the targets were not saved on this platform. Other phishing simulated study tools such as Gophish, Phishing frenzy, King phish, and Cofense (as shown in table 10.2) were not adopted in this study because they were all email-based systems and not for SMS-based attacks [79].

In terms of privacy, security, and ethical considerations, Jalili et al avoided collecting information for fear of privacy breaches. Similarly, Slonka et al did not actually harvest the credentials of the targets but replaced the provided emails with some numerical values and further used SSL to secure the connection, between the web server and the target participants. These were deemed safe methods however, we encrypted the unique click events that were recorded and saved onto our database of a website that was hosted for this exercise and follow the ethical road-map proposed by Salah et al [74]. The site was also secured with an SSL certificate to avoid data breaches. This approach was deemed reliable and valid for recording the unique click event of each respondent. To reduce the tendency of multiple recordings from one user, it was considered necessary to have reliable unique click events such that when a user happened to click the link more than once, the original click could be detected to avoid multiple recordings from one person. SHE-256 algorithm was used based on guidelines provided in General Data Protection Regulation of EU [88, 10].

10.5.4 Phishing attack risk among healthcare staff

The study recorded a click rate of 61.1% (as shown in Figure 10.6) which would be considered very high when compared with related investigations that were performed in [78] (20 .4%) and [29] (14.2%) . This answered the research question RQ3 indicating that healthcare workers are susceptible to a phishing attack in the hospital. After all, the phisher may just need a single click to launch the malicious payload. Therefore, a click rate of over 50% might have even exceeded the goal of the phisher. For better understanding, and as a means of dealing with survivorship bias, those who did not click

the link were contacted. With reference to Figure 10.6 and Figure10.8, out of 65 healthcare staff who were contacted, 17 of them provided brief feedback as to why they did not click on the link. Eleven of them regarded the message as suspicious while six of them were busy and failed to click the link. The healthcare staff who regarded the message as fake said they were not exposed to COVID-19 risk factors and so, did not believe the SMS message, implying that they would have been victims if they had been in contact with others at that time. So their suspicion was not based on their knowledge of phishing attacks, suggesting that such healthcare staff might also need treatment together with those who click the link to improve on their phishing attack resilience level. It is interesting to know that some healthcare staff (6 persons) did not click the link because they were busy with patient care as indicated in Figure 10.8. While a related study [41] identified that high workload contributes to phishing susceptibility, a recent study on healthcare security practice showed the reverse [91], where higher workload rather has a negative correlation with self-reported security behaviour risks of healthcare staff. Since it was merely a correlation, the authors did not attach a causality effect to the findings. Also, the study participants were relatively small, limiting the generalisation of their findings. Though this might be insignificant, our study points to a similar finding in this work, as six persons forgot to click the link simply because they were busy with patients.

To better understand the susceptibility of the victims, the location, expectation, and what the victims were engaged in, were collected via the questionnaire. Of those who provided this information, 56% were off duty while 44% were on duty. Additionally, 68% believed in the subject of the phishing message while 24% were curious. Some were engaged in patient care (32%), administrative duties (8%), leisure (12%), and house chores (8%).

According to Sonowal et al, curiosity, urgency, helpfulness, fear, trust and greed are among the properties often baked into the phishing messages to entice prospective victims [79]. Interestingly, a higher proportion of the victims who clicked the link were curious and some also trusted the message which was crafted to have these phishing message tones. A total of 40% (10) of healthcare staff who clicked the link, were also engaged in healthcare activities. On the other hand, of the 17 persons who did not click the link (as shown in Figure 10.8), six (35.3%) of them said they were busy. The question here is that during busy healthcare provision, who responds to the phish and who responds to the patient and why? It is possible that those healthcare staff who click the phishing link while caring for the patients were expecting such messages due to their exposure to COVID-related factors and probably did not perceive or appraise the cyber security consequences of their action. This calls for strengthening the security systems in the hospital such that access controls and alerts to suspicious links can prompt busy healthcare staff to carefully assess a link before clicking. For those who con-

tinue to care for the patient, it is possible that they prioritised the patient care over the phishing message. It could also be the case that they were not exposed to any COVID-19 related factors and felt less susceptible to the virus, and therefore had less priority for the phishing message.

10.5.5 Survivorship bias and feedback from respondents who neither clicked the link nor filled the questionnaire and those who clicked the link but failed to fill the questionnaire

Figure 10.8, shows the reasons why the healthcare staff click the link but failed to fill questionnaire item. Apparently, five persons claimed that the questionnaire were many while six victims responded that they were too busy did not have time to fill it in. In Ghana, the doctor-patient and nurse-patient ratios are far lower than the World Health Organisation (WHO) standard. For example, the doctor-patient ratio in Ghana is about 1:13,000 while that of the WHO limit is at 1:5,000 [61, 8]. This supports the findings that the healthcare staff could be busy and do not have time to fill out the questionnaire.

10.5.6 Implication of the study

Our study has both practical implications and implications for the scientific community. First of all, new knowledge has been provided in the state-of-the-arts regarding phishing simulation methods, tools, payloads, ethics, privacy, and security in the context of healthcare for future consideration. Secondly, it is now known that being busy in the hospital can disturb conscious care phishing behaviour and can equally have a positive effect on conscious care behaviour. Armed with this knowledge, security professionals can find a balance of training healthcare staff to promote their conscious care phishing behaviour. Extra security layers could also be provided in healthcare to support users in their effort of conscious care security practice, especially in the emergency department. Additionally, as PB risk positively predicted IB risk, PB risks can then be improved towards improving conscious care behaviour if causality is established. Furthermore, workload predicted SE risk in the positive direction while SE risk predicted IB risk in the negative direction.

Based on this study, various measures need to be taken by the leaders of healthcare and even the government in the area of phishing attack. The leaders of the healthcare need to provide appropriate training, awareness,learning and eduction to averse this susceptibility trend. Also, Intrinsic incentives can be designed based on these findings to improve phishing related conscious care behaviour.For instance, regarding educating staff on

phishing attack, the healthcare staff need to know how to comprehensively identify phishing clues. This could provide them with the knowledge to avoid clicking on suspicious links. After educating the staff, training with simulation attacks need to be conducted with the healthcare staff to help them to understand the nature of real attacks. Aside these, the perception of the healthcare staff need to improve to reduce the security behaviour risk. This ca, social and cultural factors need to be developed to improve on the conscious care behaviour of the healthcare staff. Equipping the healthcare staff with adequate knowledge and skills sound phishing related security practice, could be reducing the perceived barrier risk in phishing attack and other perception risks. In this regards, state-of-the-art training technologies such as virtual reality, augmented reality or extended reality could be employed to train and inculcate longer lasting psychological incentive towards avoidance of phishing susceptibility. In traditional training methods, people may skip through online modules reading the bare minimum to pass the final quiz, Or attend a presentation without really paying attention or absorbing any knowledge. Virtual realities may not only enable people not only to see and understand the problem of cybersecurity relating to phishing, but will engage them emotionally. Immersive technologies are deemed effective. For instance, a study by Kohn et al showed that when students are engaged and motivated such that they feel less stress, the understanding of what they are being thought is better and they experience better levels of cognition, develops patterns, and experience better long lasting in memory [26].

In the simulated attack, the SMS message caption was crafted to originate from the government institution responsible for healthcare. This could have also increased the click rate since some of the healthcare staff will not doubt the source. There, the government should prevent SMS services providers platforms to use the names of reputable companies as sources of SMS message. This way, adversaries will try to create similar names of related companies but not exact. This could help increase the suspicion of the source of SMS messages by the targets and can help to reduce the susceptibility level of phishing attack.

10.5.7 Conclusion

Following the huge benefits of ICT systems in healthcare, many hospitals have abandoned paper-based systems for computerised systems. However, the associated challenges include ransomware attacks and other cybersecurity-related threats. A phishing attack happens to be the most common method of ransomware attack because it targets at the most vulnerable link in the security chain.

Guided with state-of-the-art and observational measures, an SMS-based phishing simulation study was performed among healthcare workers in

Ghana who elected to be part of the study. The results showed that more than half of the targeted healthcare staff (61%) were susceptible. To prevent survivorship bias, a phone call conversation showed that some of the healthcare staff were not victims in the attack because they prioritised patient care and were not susceptible to the simulated phishing attack. The self-reported phishing behaviours of healthcare workers were generally lower than their actual behaviour of having clicked the link. A correlation between work factor variables and perception variables showed that perceived barrier is a predictor of self-reported intended behaviour among healthcare staff, workload significantly predicted self-efficacy risk (r = 0.494, p-value = 0.05), and work emergency predicted perceived barrier risk in the reverse direction at a significant level (r = -0.401, p-value = 0.05). Furthermore, , Self-efficacy negatively predicted self-reported security behaviour related to phishing attack. If causality was established, it basically would have meant that, healthcare staff are confident in their ability to appraise and avoid phishing attacks but do not in fact have the requisite ability to overcome them. Various suggestions have been provided to the leaders of the healthcare organization in Ghana and the government, towards reducing phishing susceptibility level in the healthcare. For instance, state-of-the-art training, by using immersive technologies including virtual reality, could help to improve on the psychological perceptions (such as perceived barrier and self-efficacy) that have higher risk to cyber security practice. Some suggestions have also been provided to the government, regarding how to reduce the issue of cyber criminals being able to use the names of reputable organizations in SMS-based phishing attack.

One of the limitations in this study includes the small number of participants who responded to the questionnaire. We pretested our questionnaire, but future studies could therefore conduct a more intensive pre-testing to increase the response rate. Additionally, further work is needed to practically assess the treatment effects with multiple clicks to practically assess various incentives such as the perception variables in HBM, PMT and cognitive dissonance in phishing simulation study. Guided with these perception and work factors that affect the phishing security practice, better security training, awareness, and incentive measures can therefore be crafted in order to mitigate the phishing susceptibility rate.

10.6 Appendix 1

10.7 Bibliography

[1] ABDELHAMID, M., ET AL. The role of health concerns in phishing susceptibility: Survey design study. *Journal of medical Internet research* 22, 5

(2020), e18394. 15, 272, 284, 285, 297, 491

[2] ADU, E. K., MILLS, A., AND TODOROVA, N. Factors influencing individuals' personal health information privacy concerns. a study in ghana. *Information Technology for Development 27*, 2 (2021), 208–234. 270

[3] ANAWAR, S., KUNASEGARAN, D. L., MAS'UD, M. Z., AND ZAKARIA, N. A. Analysis of phishing susceptibility in a workplace: a big-five personality perspectives. *J Eng Sci Technol 14*, 5 (2019), 2865–2882. 294

[4] ANDERSON, J. C., AND GERBING, D. W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin 103*, 3 (1988), 411. 295

[5] ANSARI, Z. M., YASIN, H., ZEHRA, N., AND FAISAL, A. Occupational stress among emergency department (ed) staff and the need for investment in health care; a view from pakistan. *Journal of Advances in Medicine and Medical Research* (2015), 1–9. 11, 273

[6] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., AND XU, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. 272, 274, 296, 313, 404, 406, 412, 414, 442, 444, 457, 512

[7] ATHANASSOULIS, N., AND WILSON, J. When is deception in research ethical? *Clinical Ethics 4*, 1 (2009), 44–49. 282, 283, 498

[8] ATINGA, R. A., ABEKAH-NKRUMAH, G., AND DOMFEH, K. A. Managing healthcare quality in ghana: a necessity of patient satisfaction. *International Journal of Health Care Quality Assurance* (2011). 300

[9] AYAKWAH, A., DAMOAH, I. S., AND OSABUTEY, E. L. Digitalization in africa: The case of public programs in ghana. In *Business in Africa in the Era of Digital Technology*. Springer, 2021, pp. 7–25. 270

[10] BAIG, A. Understanding data encryption requirements for gdpr, ccpa, lgpd & hipaa, 2020. Available from: "https://www.thesslstore.com/blog/understanding-data-encryption-requirements-for-gdpr-ccpa-lgpd-hipaa/". 298

[11] BALL, R., AND WATTS, R. Some additional evidence on survival biases. *The Journal of Finance 34*, 1 (1979), 197–206. 282

[12] BARRACUDA. Barracuda phishline:fight phishing with continuous simulation and training, January 2022. Available from: https://www.barracuda.com/resources/Barracuda_PhishLine_DS_U. 286

[13] BOLLEN, K. A., AND PEARL, J. Eight myths about causality and structural equation models. In *Handbook of causal analysis for social research*. Springer, 2013, pp. 301–328. 295

[14] CAMPBELL, C. C. Solutions for counteracting human deception in social engineering attacks. *Information Technology & People* (2019). 284

[15] CAZARES, M. F., ARÉVALO, D., ANDRADE, R. O., FUERTES, W., AND SÁNCHEZ-RUBIO, M. A training web platform to improve cognitive skills for phishing attacks detection. In *Intelligent Sustainable Systems*. Springer, 2022, pp. 33–42. 272, 495

[16] CHAMPION, V. L., SKINNER, C. S., ET AL. The health belief model. *Health behavior and health education: Theory, research, and practice 4* (2008), 45–65. 9, 272, 496

[17] CHAUDHRY, J. A., CHAUDHRY, S. A., AND RITTENHOUSE, R. G. Phishing attacks and defenses. *International Journal of Security and Its Applications 10*, 1 (2016), 247–256. 19, 297

[18] CHEN, Y., NYEMBA, S., ZHANG, W., AND MALIN, B. A. Specializing network analysis to detect anomalous insider actions. *Security Informatics 1*, 1 (2012), 5. 140, 272

[19] CHEN, Y., XIA, W., AND COUSINS, K. Voluntary and instrumental information security policy compliance: an integrated view of prosocial motivation, self-regulation and deterrence. *Computers & Security 113* (2022), 102568. 272, 495

[20] CHERNYSHEV, M., ZEADALLY, S., AND BAIG, Z. Healthcare data breaches: Implications for digital forensic readiness. *Journal of medical systems 43*, 1 (2019), 1–12. 270

[21] COCKER, F., AND JOSS, N. Compassion fatigue among healthcare, emergency and community service workers: A systematic review. *International journal of environmental research and public health 13*, 6 (2016), 618. 11, 273

[22] COFENSE. Security solutions built to stop phish, January 2022. Available from: `https://cofense.com/`. 286

[23] FADDIS, A. The digital transformation of healthcare technology management. *Biomedical instrumentation & technology 52*, s2 (2018), 34–38. 270

[24] FALK, R. F., AND MILLER, N. B. *A primer for soft modeling*. University of Akron Press, 1992. 295

[25] FLORES, W. R., HOLM, H., SVENSSON, G., AND ERICSSON, G. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security* (2014). 284

[26] GALLAGHER, A. G., AND CATES, C. U. Virtual reality training for the operating room and cardiac catheterisation laboratory. *The Lancet 364*, 9444 (2004), 1538–1540. 301, 510

[27] GETGOPHISH. Open-source phishing framework, January 2022. Available from: `https://getgophish.com/`. 286

[28] GOEL, S., WILLIAMS, K., HUANG, J., AND WARKENTIN, M. Understanding the role of incentives in security behavior. 294

[29] GORDON, W. J., WRIGHT, A., AIYAGARI, R., CORBO, L., GLYNN, R. J., KADAKIA, J., KUFAHL, J., MAZZONE, C., NOGA, J., PARKULO, M., ET AL. Assessment of employee susceptibility to phishing attacks at us health care institutions. *JAMA network open 2*, 3 (2019), e190393–e190393. 11, 14, 15, 200, 272, 280, 284, 285, 297, 298, 492

[30] GORDON, W. J., WRIGHT, A., GLYNN, R. J., KADAKIA, J., MAZZONE, C., LEINBACH, E., AND LANDMAN, A. Evaluation of a mandatory phishing training program for high-risk employees at a us healthcare system. *Journal of the American Medical Informatics Association 26*, 6 (2019), 547–552. 14, 15, 200, 272, 284, 285, 297, 491, 492

[31] HAIR, J. F., PAGE, M., AND BRUNSVELD, N. *Essentials of business research methods*. Routledge, 2019. xx, 294, 415, 501, 502

[32] HENSELER, J., RINGLE, C. M., AND SARSTEDT, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science 43*, 1 (2015), 115–135. 295

[33] HOULE, D. High enthusiasm and low r-squared, 1998. 295

[34] HOXHUNT. Enterprise security awareness,re-invented, January 2022. Available from: `https://www.hoxhunt.com/`. 286

[35] HUMAIDI, N., AND BALAKRISHNAN, V. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR* (2012), vol. 35, IACSIT Press Singapore, pp. 1–6. 12, 15, 200, 272, 274

[36] HUMAIDI, N., BALAKRISHNAN, V., AND SHAHROM, M. Exploring user's compliance behavior towards health information system security policies based on extended health belief model. In *2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)* (2014), IEEE, pp. 30–35. 9, 273, 274, 496, 509

[37] IFINEDO, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security 31*, 1 (2012), 83–95. 10, 273, 457, 496

[38] IFINEDO, P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management 51*, 1 (2014), 69–79. 313, 512

[39] INFOSECINSTITUTE. Prepare every employee with phishing simulations & training, December 2021. Available from: https://www.infosecinstitute.com/iq/phishing/. 286

[40] IRONSCALES. Phishing simulation & training:anti phishing simulations and customized training based on real-time data and real world situations., January 2022. Available from: https://ironscales.com/solutions/threat-assessment/phishing-training/. 286

[41] JALALI, M. S., BRUCKES, M., WESTMATTELMANN, D., AND SCHEWE, G. Why employees (still) click on phishing links: investigation in hospitals. *Journal of medical Internet research 22*, 1 (2020), e16775. 11, 15, 272, 273, 274, 280, 282, 284, 285, 295, 296, 297, 299, 312, 313, 445, 491, 492, 508

[42] KENNEDY, D. Introducing spearphisher – a simple phishing email generation tool, January 2022. Available from: https://www.trustedsec.com/blog/introducing-spearphisher-simple-phishing-email-generation-tool/. 286

[43] KNOWBE4. Phishing, January 2022. Available from: https://www.knowbe4.com/phishing. 286

[44] LEGUINA, A. A primer on partial least squares structural equation modeling (pls-sem), 2015. 295

[45] LI, Y., XIONG, K., AND LI, X. Understanding user behaviors when phishing attacks occur. In *2019 IEEE international conference on intelligence and security informatics (ISI)* (2019), IEEE, pp. 222–222. 284

[46] LUCY. Cyber security training solutions, January 2022. Available from: https://lucysecurity.com/. 286

[47] MCELWEE, S., MURPHY, G., AND SHELTON, P. Influencing outcomes and behaviors in simulated phishing exercises. In *SoutheastCon 2018* (2018), IEEE, pp. 1–6. 284

[48] MIMECAST. Relentless protection starts here, January 2022. Available from: https://www.mimecast.com/. 286

[49] MISHRA, S., AND SONI, D. Sms phishing and mitigation approaches. In *2019 Twelfth International Conference on Contemporary Computing (IC3)* (2019), pp. 1–5. 271

[50] MOHAMED, N., AND AHMAD, I. H. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from malaysia. *Computers in Human Behavior 28*, 6 (2012), 2366–2375. 313, 512

[51] MOROLONG, M. P., SHAVA, F. B., AND SHILONGO, V. G. Designing an email security awareness program for state-owned enterprises in namibia. In *IOT with Smart Systems*. Springer, 2022, pp. 679–688. 297

[52] MOU, J., COHEN, J. F., BHATTACHERJEE, A., AND KIM, J. A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems 23*, 1 (2022), 196–236. 10, 273, 457, 496

[53] NASSER, G., MORRISON, B. W., BAYL-SMITH, P., TAIB, R., GAYED, M., AND WIGGINS, M. W. The role of cue utilization and cognitive load in the recognition of phishing emails. *Frontiers in big Data 3* (2020), 33. 293

[54] NEWS, B. S. H. I. Ransomware is leading hospital boards to pour more money into cybersecurity, October 2021. Available from: https://www.healthcareitnews.com/news/ransomware-leading-hospital-boards-pour-more-money-cybersecurity. 270, 442

[55] NG, B.-Y., KANKANHALLI, A., AND XU, Y. C. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 4 (2009), 815–825. 9, 271, 272, 273, 296, 313, 442, 496, 509, 512

[56] NIFAKOS, S., CHANDRAMOULI, K., NIKOLAOU, C. K., PAPACHRISTOU, P., KOCH, S., PANAOUSIS, E., AND BONACINA, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors 21*, 15 (2021), 5119. 270

[57] OF OSLO, U. Web form for questionnaire registrations, January 2022. Available from: https://nettskjema.no/. 280

[58] OF PUBLIC HEALTH, B. U. S. Behaviour change models:the health belief model, January 2022. Available from: https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/behavioralchangetheories2.html. 271

[59] ÖĞÜTÇÜ, G., TESTIK, Ö. M., AND CHOUSEINOGLOU, O. Analysis of personal information security behavior and awareness. *Computers & Security 56* (2016), 83–93. 284

[60] ON PRIMARY HEALTH CARE, W. H. O. W. Technical series on primary healthcare, June 2021. Available from: https://www.who.int/docs/default-source/primary-health-care-conference/digital-technologies.pdf?sfvrsn=3efc47e0_2. 270

[61] OPOKU, S. Y., BENWELL, M., AND YARNEY, J. Knowledge, attitudes, beliefs, behaviour and breast cancer screening practices in ghana, west africa. *Pan African Medical Journal 11*, 1 (2012). 300

[62] OSEI, E., AGYEI, K., TLOU, B., AND MASHAMBA-THOMPSON, T. P. Availability and use of mobile health technology for disease diagnosis and treatment support by health workers in the ashanti region of ghana: A cross-sectional survey. *medRxiv* (2021). 270

[63] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., AND ZWAANS, T. The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security 66* (2017), 40–51. 10, 278, 404, 405, 406, 408, 413, 414, 415, 426, 428, 443, 446, 499, 501, 502

[64] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. The development of the human aspects of information security questionnaire (hais-q). 7, 10, 278, 282, 414, 442, 443, 446, 461, 498

[65] PHISHER, K. King-phisher, January 2022. Available from: https://www.kali.org/tools/king-phisher/. 286

[66] PHISHING FRENZY. Phishing all the chings, January 2022. Available from: https://www.phishingfrenzy.com/. 286

[67] PRIESTMAN, W., ANSTIS, T., SEBIRE, I. G., SRIDHARAN, S., AND SEBIRE, N. J. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics 26*, 1 (2019). 11, 15, 272, 284, 285, 297, 492

[68] PRISMA. Systematic reviews: Step 8: Write the review, 2018. xiv, 284, 337

[69] PROOFPOINT. Attackers start with people. your cybersecurity strategy should too., January 2022. Available from: https://www.proofpoint.com/us. 286

[70] RAKHRA, M., AND KAUR, D. Studying user's computer security behaviour in developing an effective antiphishing educational framework. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (2018), IEEE, pp. 832–836. 284

[71] RHEE, H.-S., KIM, C., AND RYU, Y. U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security 28*, 8 (2009), 816–826. 313, 512

[72] RINGLE C. M., W. S., AND BECKER. "smartpls 3.", 2015. Available from: "http://www.smartpls.com.". 295

[73] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 9, 10, 12, 15, 200, 274, 405, 407, 412, 428, 446, 457

[74] SALAH EL-DIN, R. To deceive or not to deceive! ethical questions in phishing research. 278, 282, 283, 297, 298, 498

[75] SHAH, M. Perception of managers on the effectiveness of the internal audit functions: A case study in tnb. xx, 294, 415, 501, 502

[76] SHIH, D.-H., LIN, B., CHIANG, H.-S., AND SHIH, M.-H. Security aspects of mobile phone virus: a critical survey. *Industrial Management & Data Systems* (2008). 313, 512

[77] SIEBER, J. E. Deception in social research i: Kinds of deception and the wrongs they may involve. *IRB: Ethics & Human Research 4*, 9 (1982), 1–5. 282, 498

[78] SLONKA, K. J., AND SHRIFT, B. F. Phishing our clients: A step toward improving training via social engineering. *Issues in Information Systems 17*, 1 (2016). 14, 15, 272, 284, 285, 297, 298, 491

[79] SONOWAL, G. Phishing kits. In *Phishing and Communication Channels*. Springer, 2022, pp. 115–135. 271, 280, 298, 299

[80] SPENCE, N., PAUL, D. P., AND COUSTASSE, A. Ransomware in healthcare facilities: The future is now. 270

[81] SPF. Spf – speed phishing framework, January 2022. Available from: https://sectechno.com/spf-speedphishing-framework/. 286

[82] SPTOOLKIT. sptoolkit rebirth – simple phishing toolki, December 2021. Available from: https://www.darknet.org.uk/2015/04/sptoolkit-rebirth-simple-phishing-toolkit/. 286

[83] STATOLOGY. What is a good r-squared value?, 2019. Available from: "https://www.statology.org/good-r-squared-value/". 295

[84] STEWART, H., AND JÜRJENS, J. Information security management and the human aspect in organizations. *Information & Computer Security* (2017). 293

[85] TRUSTEDSEC. The social-engineer toolkit (set), January 2022. Available from: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/. 286

[86] ULFATH, R. E., SARKER, I. H., CHOWDHURY, M. J. M., AND HAMMOUDEH, M. Detecting smishing attacks using feature extraction and classification techniques. In *Proceedings of the International Conference on Big Data, IoT, and Machine Learning* (2022), Springer, pp. 677–689. 271

[87] VERIZON2021. 2021 data breach investigations report, November 2021. Available from: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf. 1, 270, 293, 441, 454

[88] YENG, P., WOLDAREGAY, A. Z., AND HARTVIGSEN, G. K-cusum: Cluster detection mechanism in edmon. 25, 217, 234, 249, 298

[89] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[90] YENG, P. K., D., S., AND YANG, B. Legal requirements towards enhancing the security of medical devices. 270

[91] YENG, P. K., FAUZI, M. A., AND YANG, B. Assessing the effect of human factors in healthcare cyber security practice: An empirical study. In *25th Pan-Hellenic Conference on Informatics* (2021), pp. 472–476. 299

[92] YENG, P. K., SZEKERES, A., YANG, B., AND SNEKKENES, E. A. Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: Systematic mapping study. *JMIR human factors 8*, 2 (2021), e17604. 9, 11, 15, 17, 24, 272, 273, 274, 282, 405, 406, 407, 414, 457, 496, 498

[93] YENG, P. K., WOLDAREGAY, A. Z., AND HARTVIGSEN, G. K-cusum: Cluster detection mechanism in edmon. 270

[94] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 11, 15, 22, 138, 200, 217, 224, 236, 273, 274, 404, 406, 407, 409, 414, 426, 442, 491, 498

[95] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: A literature survey. *Studies in health technology and informatics 261* (2019), 239–245. 273, 278, 496

[96] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 1, 2, 6, 10, 11, 15, 17, 23, 199, 217, 224, 274, 282, 404, 405, 406, 407, 409, 410, 414, 442, 443, 454, 457, 491, 498

Table 10.8: Principal findings

No	Research Question (RQ) and Hypothesis(H)	Principal finding	Remark
1	RQ1	• Six scientific papers were identified in this study as shown in table 10.2 • Five of them employed in-the-wild field study. • One of the of the study used only survey while Jalili et al adopted both survey and in the wild study[41] • Only Jalili et al conducted their study based on theories ie PMT and collective felt truth [41]. • Five of the studies used email based study. • Third party tools and custom-developed tools were used in this work. • 16 phishing simulation tools were also identified as shown in table 10.3	
2	RQ2	• Avoid collecting sensitive information from participants • Encrypt data received from participants • Avoid using actual malicious links	
3	RQ3	102 (61.1%) healthcare staff clicked the simulated malicious	
4	RQ4	• Some staff were busy and did not click the link, • Others suspected the message to be fake. • Seven (68%) out of the 25 participants believed in the subject of the phishing message • Six (24%) were curious	
5	RQ5	Self reported behaviour and perception risks were generally lower than their actual behaviour as shown in figure 10.9	
6	RQ6	Deceptiveness can be used in research but certain procedures need to follow. These include: • Pre-launch procedure • Consideration of data protection • Consideration of well-being of participants • Perform debriefing • Provide post-inform consent	
7	H1	Significant estimate (value -0.46, p-value = 0.00) between work emergency and perceived barrier	This was confirmed with Pearson's correlation coefficient (-0.494, p-value = 0.00)
8	H10	Significant estimate (value 0.5, p-value=0.02) between workload and self-efficacy	This was confirmed with Pearson's correlation coefficient value 0.494, p-value=0.05)

Table 10.9: Questionnaire items.

No	Item	Construct	Ref
1	It is inconvenient to check the security of an email with attachment	PB	[6, 55]
2	I do not have the time to check for phishing clues in an email		
3	I do not have the knowledge to check for phishing clues in an email		
4	I have not been trained properly to identify phishing related clues		
5	My hospital can not be hacked if I click on a malicious link	PV	[50, 55, 6]
6	Loss of data resulting from hacking is a serious problem for my hospital		
7	Giving out my password and username to external person can lead to unauthorized access in my hospital systems		
8	My hospital can be attacked by ransomware if I click on a malicious link		
9	I have the skills to identify malicious or phishing links in emails	SE	[71, 38, 55]
10	I am confident that I cannot download malicious attachment		
11	I am confident that I cannot share my username and password with others through phishing attack		
12	I am confident that I will not download malicious software on my computer		
13	I feel that my chance of receiving an email attachment with a virus is high	PS	[6, 55]
14	I feel that I could fall victim to a malicious attack if i fail to comply with my organization's information security policy		
15	My organization's data and resources may be compromised if I don't pay adequate attention to phishing attack tricks		
16	It is not likely that an information security breach can occur at my workplace through clicking email links		
17	I check the links in my email or SMS to be sure it is not harmful before clicking	IB	[6, 55, 76]
18	I do not open email attachments from people whom I do not know		
19	I do not enter usernames, passwords and other sensitive information on pop-up windows		
20	**I always verify the source of the email or SMS before accessing its content**		
21	**I was called to attend to urgent issues prior to clicking the link**	WE	
22	Prior to clicking the link, the work i was performing required URGENT or IMMEDIATE intervention to prevent a worsening condition which poses an immediate risk to health and life		
23	I was called outside my shift time to attend to urgent issues prior to clicking the link		
24	**I was preparing to receive an emergency case prior to clicking the link**		
25	In my workplace, I SKIPPED my daily break or I was in a hurry in order to keep up with my workload prior to clicking the link	WL	[41]
26	**I was at work early or I stayed late outside of my regular or normal working hours in order to keep up with my workload prior to clicking the link**		
27	Prior to clicking this link, I had performed some mind draining activities (thinking, deciding, calculating, remembering, looking, searching, etc.) which affected my ability to pay much attention to the message details and the SMS links before clicking.		
28	**Prior to clicking this link, I had performed some amount of physical activities (e.g., pushing, pulling,turning, controlling, activating, etc.) which affected my ability to pay much attention to message details and the SMS link before clicking.**		

Part IV

Psychological, social and cultural (PSC) factors

Studies in Health Technology and Informatics 2019 ;Volum 261. s. 239-245
The publication is available at IOS Press through https://doi.org/10.3233/978-1-61499-975-1-239

Chapter 11

Healthcare Staffs' Information Security Practices Towards Mitigating Data Breaches:Literature Survey

Prosper Kandabongee Yeng, Bian Yang and Einar Arthur Snekkenes

Abstract

The purpose of this study was to understand healthcare staffs' information security (IS) practices towards mitigating data breaches. A literature survey was conducted to understand the state-of-the-art methods, tools, evaluation techniques and the challenges to their implementation. The results would be used for empirical studies in a hospital setting in Norway on Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI). The human Aspect of the Information Security Questionnaire was identified as robust and comprehensive tool for gathering staff security practices. Integrated theories was being adopted to form comprehensive staffs' characteristics. A mixed-method for evaluating the theories was also identified to be the best strategy.

11.1 Introduction

The healthcare sector depends heavily on ICT for telemedicine services, electronic health records management and decision support among others. The use of this technology generates huge variant data and drives the connection of services and data with many users including patients, healthcare providers, systems and devices. Attack surfaces of ICT systems have hence been increased and become honey pots, attracting malice [18]. For instance, in 2018, through the aid of a staff, the South-East Regional Health Authority's health records of about half the total population of Norway (3 million) were compromised [12]. Healthcare data is richer than data in the financial sector and it costs ten times more than credit card data from banks in the underground cyber markets[13]. The healthcare data can be used to commit multiple identity theft including the generation of fraudulent medical insurance claims, fake identity cards to procure medicines and medical devices

[23]. Stolen healthcare data can also be used to obtain medical treatment and gain access to credit card information [23]. Perimeter defenses have been heightened by physical security systems and technological countermeasures such as firewalls, intrusion detection and prevention systems, security policy configurations and antivirus systems [30]. With humans being the most vulnerable link in the security chain, attackers turn to explore this and gain ingress into the systems. Healthcare staffs' practices can also deliberately or inadvertently cause internal security breaches [18] and the consequences ranges from fraud to loss of human lives [20] and fines up to Twenty Million Euros[10]. The annual estimated losses from cybercrime is forecasted to reach USD 2 trillion from few years to come [14]. Though security in healthcare extend beyond ICT-related systems [14], this current study is limited to healthcare security in ICT. Poor security practices have been realized to be influenced by individual characteristics including social demographics and psycho-socio-cultural factors [26]. Healthcare staffs' security practices relate to individual staff's personal characteristics such as social demographics, psycho-socio-cultural behavior and access control management of employees [8]. Socio-demographic characteristics in this study include age, gender, education, workload level, emergency situation and security experience while psycho-socio-cultural characteristics in this study are referred to personal behaviors that are influenced by psychological, social and cultural factors including perception, attitude, norms and beliefs [3]. Other healthcare staff security practices which impact security but are beyond the scope of this study are organizational culture and motivation. In using healthcare information systems, employees' practices, induced by their characteristics, may have a positive or negative impact on information security (IS) [6]. Password management, physical security measures, how users respond to phishing attacks and how users handle resources entrusted to them by their user credentials and access, are some instances of employee security practices [**?**]. Healthcare staff are required to be confidential with patients' information [5], however, the analysis of their conduct is beyond the scope of this paper. Healthcare staffs' security practices are deemed to be tracked in access control systems however, this paper is focused on healthcare staffs practices in the context of socio-demographics and psycho-socio-cultural practices. Healthcare staff and employees have been adopted in this study to be synonymous and were used interchangeably. The healthcare staff in this study were limited to personnel who accesses PHI for therapeutic, health financing and other healthcare-related reasons. The general objective was to conduct a literature survey for the state-of-the-art theories, holistic security practices and efficient evaluation strategies. The results would be used to conduct a holistic and empirical study to unearth how social bonding, work-group peer influences, societal norms and beliefs, healthcare emergency situations, workload, security perceptions, age, gender and experi-

ence influence information security in healthcare. The results are intended to promote good security practices in the healthcare sector in Norway, by using incentivization measures. The state-of-the-art theories would be used to obtain comprehensive characteristics and practices of healthcare staff which often have a significant impact on security.

11.2 Method

A literature survey was explored as an initial effort to understand the research area under the Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) project which is operated by the Centre of Cyber and Information Security of NTNU and funded by the Ministry of Health and Care of Norway. IEEE-Xplore, Google Scholar, Elsevier and Science Direct were searched for journals and conference papers in behavioural theories and healthcare staffs security practices. Only studies which implemented and evaluated these theories were included in the survey. The results were critically analyzed, appraised and classified under the HSPAMI study area as shown in Table 1. The study was organized into state-of-the-art relating to modeling staffs' characteristics, staffs' security practices and evaluation techniques.

11.3 Results

11.3.1 State-of-the-art studies relating to Modelling staffs' characteristics

Healthcare staffs are characterized with social bonding, privacy and security perceptions, emotions and their work is often associated with high workload and emergency cases among others [5]. The significance of these traits could undermine IS policies and regulations which can lead to IS violations [5]. Through a systematic review, Lebek et al. discovered Theory of Reasoned Action (TRA) /Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM) as the most used theories for studying human security practices in the psycho-socio-cultural context [6]. Lebek et al. provided knowledge in common theories which can be used in HSPAMI but, guidelines were not provided on the selection and application of these theories. Cheng et al. [6] combined social control (SC) and GDT to study employee security behavior including peer pressures among co-workers. Perceived severity and norms of the work environment were found to have a significant impact on the intentions of IS violations but not perceived sanctions. Social factors and fear were considered in the combined study however, personality, emotions, economic and prior experience were not consid-

ered in the combined framework [25]. Furthermore, a Health Belief Model (HBM) [21] was used to survey 134 staffs of different organizations in Singapore. The results showed that perceived susceptibility, benefits, and self-efficacy has influence on email-related security behavior. HBM addresses security issues relating to cognitive theory of motivation and beliefs but it does not consider attitudes, personality, environmental, economic, prior experience and social influences. McCormac et al., explored the relationship between IS Awareness (ISA) and personality with 505 working Australians among other traits with the Big Five model (TBF)[19]. There were significant positive correlation relationships between conscientiousness (r =0.56, p ¡ 0.001), agreeableness (r = 0.49, p ¡ 0.001), openness (r = 0.19, p ¡ 0.001) and ISA. In TBF theory [27], personality traits are stable over time and they can hence be used for long-term prediction of security practices than attitude. However, TBF employs self-assessment which could lead to skewness of results emanating from confirmation bias. Socio-demographic traits are also useful in the coalition of staffs' characteristics towards an effective study [3, 19]. Anwa et al. [3] showed that gender has some effect in security self-efficacy (r=-.435, p¡ .001), experience (r=-.235, p¡ .001) and computer skills (r=-.198, p¡ .001) but minimal effect in cues-to-action (r=-.152, p¡ .001) and self-reported cybersecurity behaviors (r=-.152, p¡ .001) [3]. Roer et al.,, conducted a security culture study in Norway and Sweden among 10,000 employees across different industries [15]. In the report, 23.0% of men have negative security practice as against 15.3% of women. About 11.2% of men have bad password management behavior than women (6.6%). Men have more negative behavior towards security policies than women in the study. Anwa et al., and Roer et al., provided knowledge on the impact of demographic variables but they did not explore the influence of psycho-socio-cultural variables with the demographics.

11.3.2 State-of-the-art studies relating to Staffs' security practices

In modeling human behavior with these theories, the independent variables such as the staffs' associated characteristics, are often explored with the dependent variables such as the staffs' security practices [25, 21]. There is therefore the need to have comprehensive security practices which are most prone to security violations, compliance and represent all sections of an information security policy that are essential to safeguard the CIA [22]. Various studies adopted security practices in isolation or limited combination such as password management, discarding confidential information, ensuring the privacy of personal information and reporting security violation in a clinical setting [6, 3, 5, 21]. Other studies including relied on Authentication, De-Authentication and Permission Management. However, these security practices alone do not constitute a holistic policy requirement [22] and are not comprehensive enough. McCormac, et al., used a comprehensive tool

known as the human aspect of information security questionnaire (HAIS-Q) in determining individual differences and IS awareness. This tool consists of all aspect of IS policy behaviors relating to staffs' practices [27]. HAIS-Q security practices includes internet use, email use, social media use, password management, incident reporting, information handling and mobile computing [27]. But the tool is required to always be updated to reflect current IS standards and policies prior to usage [27].

11.3.3 State-of-the-art-studies relating to Evaluation Techniques

On the part of the evaluation of these theories, most of the studies, [6, 3, 5, 21], used a survey with only questionnaire instrument in a quantitative study. A study was conducted in a healthcare setting [16] used only interview and observational methods in a qualitative study. Rezgui, et al., employed interviews, questionnaires and observations [24] in a mixed method. The main merit of quantitative method approaches to qualitative analysis is that the findings can be implemented in other types of populations with the same degree of certainty that qualitative approaches have. But the qualitative methods also provide room for clarifications of ambiguities [24]. In summary, the various theories were categorised into some aspects of HSPAMI study areas as shown in Table **??**.

Table 11.1: Analysis of the theories and their application areas in HSPAMI

HSPAMI study area	**Theories that support study area**
Social Bonding (SB)	SC [6]
Peer Pressure (PP)	SC[6]
Social Norms and Beliefs (SNB)	SC, HBM [6, 21]
Healthcare Emergency (HCE)	PMT, SC, TPB [6, 26, 17]
Work Load (WKL)	PMT, HBM [21, 17]
Privacy and Security perception	PMT, DT, HBM [6, 21, 17]
Personality and Attitude (PA)	TBF, TPB, HBM [26, 21, 27]
IS Experience, Education and Knowledge (IEEK)	PMT [21]
Emotions	PMT, HBM [26, 21]

11.4 Discussion

The general objective was to conduct a literature survey for the state-of-the-art theories, security practices and evaluation strategies of the theories. The results of the theories were analyzed into their applicable areas in HSPAMI

as shown in Table1. The HBM deals with the "subjective risks of contracting a condition" [21, 29]. For instance, in preventive healthcare behavior, a person observes a healthy diet to avoid heart-related conditions. This can be compared to an IT security practice of using a strong password to prevent unauthorized access. HBM addresses security issues based on cognitive theory of motivation such as perceptions of threat, beliefs and self-efficacy to resolve the threat but it does not consider attitudes, environmental, economic, prior experience and social influences. Therefore, HBM can be applied to the privacy and security perception variable [5]. PMT deals with the ability to protect oneself based on; the perceived severity of a threatening event, the perceived probability of the occurrence, or vulnerability, the impact of the recommended preventive behaviour and perceived self-efficacy [26]. PMT primarily uses the influence of fear appeals and considers factors such as self-efficacy, response efficacy, maladaptive response and past behaviour. However, PMT has a non-consideration of personal and demographic variables and inflexible cues to action. PMT can therefore be complemented by HBM with its flexible cues to action, and comprehensive psychological and demographic variables [7]. TPB is the use of attitude, subjective norms, and perceived behavioral control to influence individual way of life [1, 2]. TPB/TRA accounts for social norms and uses perceived behavioral control to determine intention and actual security practice. But it does not account for mood, environmental, economic and prior experience. TPB also presume staffs have the needed resources and prospect to undertake a security practice irrespective of the intention. TPB assumes staffs' security practices to be of linear decision-making process and has no provision for change in a given time. Base on its strengths, TPB can be applied to SNB, HCE and WKL [26] as shown in Table 1. GDT mission is to discourage misbehaviors of others through disciplinary measures of the offenders but does not consider social, economic or environmental factors [6, 25]. GDT mission is to discourage misbehaviors of other persons through disciplinary measures of the offenders but does not consider social, economic or environmental factors [17]. GDT is deemed not effective and has not been considered in this study [6]. TAM is for modeling the acceptance and usage of technologies but does not account for social influences, threat appeals and conscious care behavior. TAM cannot also be applied to security practices being influenced by some perceptions of users such as selection of strong passwords, frequent data backup, and cautious behavior with suspicious emails [9]. Personality traits are stable over time, so it can be used for long term prediction of security practices than attitude. In TBF model, an individual will always have a measurable personality, but individuals' attitude cannot be measured against their unexperienced technology. TBF model however does not account for socio-cultural and environmental characteristics. With regards to the study objective of HSPAMI, TBF can be applied to PA variable. Social

Control considers the influence of social factors such as peer group influence, economic, environment and deterrence measures but does not take perceptions and personality into consideration. In exploring for comprehensive security practices,[26, 6, 11] validated their studies with single or a combination of practices such as passwords, discarding confidential information and reporting security violations. However, these security practices do not constitute a holistic policy requirement [22]. But HAIS-Q tool was explored in a study involiving conscientiousness, agreeableness, emotional stability and risk-taking tendency [27]. HAIS-Q tool is deemed comprehensive and consist of various aspect of IS policy behaviors relating to staffs' practices such as Internet use, Email use, Social media use, password management, incident reporting, Information handling and Mobile computing [27]. HAIS-Q can be used to model the variables in HSPAMI and it can be updated to meet the healthcare study need [22]. HAIS-Q can also be flexibly updated with more security practices from policies and standards such as ISO 27799, to meet the requirements of the study area [27, 22]. Some studies [3, 6, 15, 11] only adopted statistical surveys to provide quantitative metrics in evaluating the theories. What employees may answer on the survey questionnaire may not be what they practice [24]. An observational and interview approach would complement to validate the data on the questionnaire. Therefore, relying on the metrics of the survey alone for decision making may deviate from the ground truth. So, the additional usage of interviews and observation may provide clarifications for the respondent to provide more accurate answers. Apparently, using a different type of data collection methods and sources results in the broad scope of data which can present a full dimension of the topic under study and help resolve issues of construct validity -the degree of the measure of the tests [4]. Different sources of data for decision making is also in line with the idea of combining multiple perceptions to draw a valid conclusion [28]. The main disadvantage of multiple data collection is the cost [24] since observation may require more time [28].

11.5 Conclusion and Future Works

This literature survey was conducted to explore theories and evaluation strategies being used to efficiently study employees' healthcare Information Technology (IT) security practices (HSPAMI). The focus was to identify appropriate and comprehensive staffs characteristics through theories and models, and to determine their evaluation methods. The intention was to use the survey findings to empirically study HSPAMI towards eliminating the millions of data breaches which are occurring in the healthcare sector. HAIS-Q was identified as a robust and valid tool or framework which can be updated to obtain holistic healthcare staff security practices for studies into

HSPAMI. An integrated approach of theories such as HBM, SC, TBF, PMT, TPB would be combined to obtain the needed healthcare staff characteristics in the psycho-socio-cultural and socio-demographic traits for the study as classified in Table 1. Also, an integrated approach of combining the theories with questionnaires, interviews and observational instruments would be used to enrich the study. With this measure, the millions of healthcare data being breached would be curtailed. The results can also be applied to other healthcare security practice-related studies, but the security practices should be aligned with policy requirements.

11.6 Bibliography

[1] AJZEN, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of applied social psychology 32*, 4 (2002), 665–683. 322

[2] AJZEN, I., AND MADDEN, T. J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology 22*, 5 (1986), 453–474. 322

[3] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., AND XU, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. 318, 320, 321, 323

[4] BONOMA, T. Case research in marketing opportunities, problems, and a process. journal of marketing research. . *Journal of Marketing Research 22* (1985), 199–208. 323

[5] BOX, D., AND POTTAS, D. Improving information security behaviour in the healthcare context. *Procedia Technology 9* (2013), 1093–1103. 318, 319, 320, 321, 322

[6] CHENG, L., LI, Y., LI, W., HOLM, E., AND ZHAI, Q. Understanding the violation of is security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security 39* (2013), 447–459. 318, 319, 320, 321, 322, 323

[7] CONNER, M., AND NORMAN, P. Predicting health behaviour: Research and practice with social cognition models. 322

[8] CONNOLLY, L. Y., LANG, M., GATHEGI, J., AND TYGAR, D. J. Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security* (2017). 318

[9] DAVIS, F. D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly* (1989), 319–340. 322

[10] EUGDPR. Key changes with the general data protection regulation, 2019. Available from: https://eugdpr.org/the-regulation/. 318

[11] FERNANDEZ-ALEMAN, J. L., SANCHEZ-HENAREJOS, A., TOVAL, A., SANCHEZ-GARCIA, A. B., HERNANDEZ-HERNANDEZ, I., AND FERNANDEZ-LUQUE, L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics 84*, 6 (2015), 454–467. 323

[12] HUGHES, O. Norway healthcare cyber-attack 'could be biggest of its kind, 2022. Available from: "https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/". 317

[13] HUMER, C., AND FINKLE, J. Your medical record is worth more to hackers than your credit card, 2014. 317

[14] ISO. Health informatics information security management in health using iso/iec 27002, 2016. Available from: "https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en". 318

[15] K ROER, G. P. Indepth insights into the human factor-the 2017 security culture report. 320, 323

[16] KOPPEL, R., SMITH, S., BLYTHE, J., AND KOTHARI, V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise*. IOS Press, 2015, pp. 215–220. 321

[17] LEBEK, B., GUHR, N., AND BREITNER, M. Transformational leadership and employees' information security performance: the mediating role of motivation and climate. 321, 322

[18] MANADHATA, P. K., AND WING, J. M. An attack surface metric. *IEEE Transactions on Software Engineering 37*, 3 (2011), 371–386. 317, 318

[19] MCCORMAC, A., ZWAANS, T., PARSONS, K., CALIC, D., BUTAVICIUS, M., AND PATTINSON, M. Individual differences and information security awareness. *Computers in Human Behavior 69* (2017), 151–156. 320

[20] MOFFIT, R. E., AND STEFFEN, B. Health care data breaches: A changing landscape. *Maryland Health Care Commission* (2017), 1–19. 318

[21] NG, B.-Y., KANKANHALLI, A., AND XU, Y. C. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 4 (2009), 815–825. 320, 321, 322

[22] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. The development of the human aspects of information security questionnaire (hais-q). 320, 323

[23] PREDD, J. B., PFLEEGER, S. L., HUNKER, J., AND BULFORD, C. Insiders behaving badly. *IEEE Secur. Priv. 6*, 4 (2008), 66–70. 318

[24] REZGUI, Y., AND MARKS, A. Information security awareness in higher education: An exploratory study. *Computers Security 27*, 7 (2008), 241–253. Available from: https://www.sciencedirect.com/science/article/pii/S0167404808000485. 321, 323

[25] ROSS, E.A., . G. M. . A survey of the foundations of order (1st ed.). routledge. *American Juurnal of Sociology 9* (1896), 513–535. 320, 322

[26] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 318, 321, 322, 323

[27] SHROPSHIRE, J., WARKENTIN, M., JOHNSTON, A., AND SCHMIDT, M. Personality and it security: An application of the five-factor model. *AMCIS 2006 Proceedings* (2006), 415. 320, 321, 323

[28] STAKE, R. The art of case study research. the art of case study research. 323

[29] STANTON, J., M. P. S. K. . J. J. Behavioral information security: Two end user survey studies of motivation and security practices. 322

[30] TETZ, E. Network firewalls: Perimeter defense - dummies, July 2019. Available from: https://www.dummies.com/programming/networking/cisco/network-firewalls-perimeter-defense/. 318

Chapter 12

Mapping the Psychosocialcultural Aspects of Healthcare Professionals' Information Security Practices: Systematic Mapping Study

Prosper Kandabongee Yeng ; Adam Szekeres ; Bian Yang ; Einar Arthur Snekkenes

Abstract

Background: Data breaches in health care are on the rise, emphasizing the need for a holistic approach to mitigation efforts. Objective: The purpose of this study was to develop a comprehensive framework for modeling and analyzing healthcare professionals' information security practices related to their individual characteristics, such as their psychological, social, and cultural traits.

Methods: The case study area is a hospital setting under an ongoing project called the Healthcare Security Practice Analysis, Modeling, and Incentivization (HSPAMI) project. A literature review was conducted for relevant theories and information security practices. The theories and security practices were used to develop an ontology and a comprehensive framework consisting of psychological, social, cultural, and demographic variables.

Results: In the review, a number of psychological, social, and cultural theories were identified, including the health belief model, protection motivation theory, theory of planned behavior, and social control theory, in addition to some social demographic variables, to form a comprehensive set of professionals' characteristics. Furthermore, an ontology was developed from these theories to systematically organize the concepts. The framework, called the psychosociocultural (PSC) framework, was then developed from the various combined psychological and sociocultural attributes of the ontology. The Human Aspect of Information Security Questionnaire was

adopted as a comprehensive tool for gathering staff security practices as mediating variables in the framework.

Conclusion: Data breaches occur often in healthcare today. This frequency has been attributed to the lack of experience of health care professionals in information security, the lack of development of conscious care security practices, and the lack of motivation to incentivize health care professionals. The frequent data breaches in health care threaten the mutual trust between health care professionals and patients, which implicitly impacts the quality of the health care service. The modeling and analysis of health care professionals' security practices can be conducted with the PSC framework by combining methods of statistical survey, observations, and interviews in relation to PSC variables, such as perceptions (perceived benefits, perceived threats, and perceived barriers) or psychological traits, social factors, cultural factors, and social demographics.

12.1 Introduction

12.1.1 Background

Data breaches in health care are on the rise, emphasizing the need for a holistic approach to risk mitigation. According to IBM's 2019 report [42], the cost of data breaches in the health care sector has remained the highest among all other sectors for the past 9 years. As of 2019, health care organizations registered the highest cost of data breaches (approximately US $6.5 million), which was 60% more than the cost reported by other industries [42]. Moreover, cyberattacks in health care are believed to represent a global phenomenon. In 2018, through the aid of a staff member, the health care records of about half the total population of Norway (3 million) were compromised [22]. The attack, which was considered as one of the biggest data breaches to have occurred in Norway, was described as a targeted method to access patient data at the Health South East Hospital. As a result, Norwegian citizens wondered whether health care data controllers were adopting reliable measures to secure the massive amount of sensitive health information collected from patients. In another incident, according to HealthCare IT News [69, 88], a phishing attack compromised 38,000 patient records from Legacy Health based in Portland, Oregon in the United States. Personal data, such as patients' email accounts, demographic information, dates of birth, health insurance data, billing details, medical data, social security numbers, and driver's license information, were stolen. In a similar incident [69, 88], about 1.5 million patient records, including data of the prime minister of Singapore, were breached. It was noted that the cybercriminals began by compromising front-end workstations, giving the attackers access to privileged user credentials. The attackers then escalated privileges to obtain access to

the database. The breached data included demographic information, patient identification numbers, and medical information, such as diagnoses and test results. In the United States, about 365 breaches were reported in 2018, and hacking was the leading cause of health care data breaches, followed by other unauthorized access and disclosure incidents [81]. The use of information technology (IT) in health care (like in other sectors) has become indispensable [35]. Electronic health records now have multiple connections to health care professionals, patients, insurers, devices, and researchers [35]. The multiple points of access available to a larger number of stakeholders translates to multiple entry points and an increased attack surface. Additionally, health care professionals are usually busy with their core roles of restoring patients' health, so little attention remains for focusing on information security [24, 16, 47]. Information security is instead often ignored to allow health care professional to focus heavily on patients' timely health restoration, especially in emergency care situations. This trade-off creates opportunities for adversaries to attack and gain access to health care systems [24, 64, 65, 82]. Perimeter defenses have long been the default mechanism for providing information and network security and have therefore matured over the years. Perimeter defenses refer to securing the boundary between a company's intranet and the public network (the internet) with physical security systems and technological countermeasures, such as firewalls, intrusion detection and prevention systems, security policy configurations, and antivirus systems [87]. Penetration through these perimeter measures is deemed more difficult and requires significant resources. Hackers therefore turn to explore easy entry points. With humans being the most vulnerable link in the security chain, attackers tend to exploit the human element to gain access to systems [78, 67]. The health care context is characterized by high levels of trust between various social and peer groups [67, 13, 14]. That trust exists largely due to the identification of health care personnel through their professional training and socialization process [47]. Additionally, all health care practitioners typically value confidentiality as a result of the ethical principles and oaths, such as the Hippocratic Oath, that are core elements in health care professions [67, 13, 14]. This social and cultural bonding of health care professionals were identified as problematic for information security [67, 13, 14]. Health care professionals' practices can also deliberately or inadvertently cause internal security breaches [69, 67, 13, 14, 70]. Furthermore, health care professionals have subtle variant behavior in the usage of Information Communication Technology in health care, which can threaten the confidentiality, integrity, and availability of personal health information [13, 77, 74] . The model of confidentiality, integrity, and availability is an information security model, which was developed to provide guidance for developing security policies to meet the availability, integrity, and confidentiality requirements of the assets of organizations [13, 77, 74].

Various researchers found that two-thirds of employees have contributed to data breaches [67, 13, 14, 20] through mistakes or deliberate actions. Security issues in health care have serious consequences [24, 50, 11]. Besides the potential loss of dignity, patients' suffering may range from fraud to patient injury or death in health care–related data breaches [88, 47, 53, 29] . Hospitals also experience a loss of trust and confidence from patients and other users if they experience data breaches. When hospital operations are interrupted, the cost of recovery from breaches is very high, especially in hacking related to ransomware [85, 33]. Health care organizations can also face stringent sanctions from regulatory bodies, such as the General Data Protection Regulation (GDPR), or as a result of violating the Health Insurance Portability and Accountability Act (HIPAA) [29, 86] . Violations of privacy and security regulations, such as the GDPR, by organizations in Europe could result in fines up to 4% of their annual global turnover or 20 million euros [30]. According to the International Organization for Standardization (ISO), the annual estimated losses from cybercrime could reach US $2 trillion in the near future, with countless daily additions of new breaches [49]. To this end, there is a need to assess the security practices of the human element in order to control data breaches in health care. Good security practices have been defined in regulations, policies, standards, guidelines, and codes of conduct, which are required to be implemented with both technical and nontechnical measures. However, to what extent do users comply with the established security policies? What are the challenges often faced by health care workers in their effort to comply with the prescribed security practices while doing their work? Are these security measures in conflict with the health care professionals' health-related practices? How can the security requirements be improved for effective compliance while improving security effectiveness? How can health care workers be incentivized to better comply with security requirements while conducting their primary work? To protect the very sensitive nature of health care data, the health care domain needs to be properly modeled, assessed, and analyzed from the perspective of all possible entry points to mitigate attacks that are often associated with the psychological, social, cultural, and demographic characteristics of system users [76]. We therefore developed a comprehensive framework to uncover security issues caused by the human element termed in this paper as "health care professionals' security practices." This paper has been organized as follows. The second section includes theoretical background, where the project, theories, and security practices used in the study are described. The third section contains related work. The fourth section provides the scope and problem definition of this study. The fifth section describes our adopted method. The sixth section presents the results. The seventh section discusses the results. The eighth section concludes the present paper and provides ideas for further work.

12.1.2 Theoretical Background: Psychosociocultural Context

Amid the increasing frequency of data breaches in health care, all possible methods that can be used to model and analyze health care professionals' security activities for security metrics should be considered. To this end, the Healthcare Security Practice Analysis, Modeling, and Incentivization (HSPAMI) project was introduced to model and analyze the security practices of health care professionals with the objective of assessing the gap between required security practices and current health care security practices [87]. The findings will support the development of solutions or incentives to improve health care professionals' security behavior. The security practices of health care professionals are influenced by their personal characteristics, such as social demographics, perceptions, and other social and cultural factors. Psychological theories have been used in studies focusing on human behavior where the results could predict human information security practices [40]. Individual health care professionals' security-related behavior can also be linked to their unique activities for constructing unique profiles in access control–related logs, such as browser histories, access logs, and network and operating system logs, in the context of big data [21]. Attack and defense simulations can also reveal health care professionals' security behavioral risk levels. In using health care information systems, employees' practices, induced by their characteristics, can have a positive or negative impact on information security [18]. Password management, physical security measures, users' responses to phishing attacks, and users' handling of resources entrusted to them by virtue of their user credentials are all examples of employee security practices [88]. The psychosociocultural (PSC) framework discussed in this paper focuses on perception, social, cultural, and sociodemographic variables. Therefore, the PSC framework depends on human behavioral theories, and individual- and work-related demographics[78] for assessing behavioral gaps in health care professionals' security practices. Information security issues in health care can no longer be mitigated by technological countermeasures alone because the problem stems from health care professionals' security practices, so enhancing "human firewalls" is necessary to mitigate the problem [82]. A human firewall involves strengthening the conscious security behavior of health care workers in order to avoid security malpractices, such as falling victims to social engineering tricks. Strengthening the conscious security behavior would augment the technological countermeasures, which would then enhance the overall security situation in health care. Frameworks for modeling and analyzing users' security practices require comprehensive behavioral theories to study health care professionals' practices for the related security metrics and to identify potential mitigation strategies. Significant information security issues relating to psychological, sociocultural, and demographic factors could undermine information security policies and regu-

lations, which could lead to information security violations [13]. Psycho-socio-cultural characteristics in this study refer to personal aspects, such as perceptions, attitudes, norms, and beliefs, as well as social and cultural factors that can influence the security practice of health care professionals [24]. Sociodemographic characteristics in this study include age, gender, education, workload level, work emergency situation, and security experience, while psychological, social, and cultural characteristics as a whole refer to health professionals' security behaviors that are influenced by their psychological, social, and cultural factors, such as perceptions, workplace peer pressure, attitudes, norms, social bonding, and beliefs [53]. In a security practice analysis, the identified theories are usually related with various security practices. -Peasons et al identified internet use, email use, social media use, password management, incident reporting, information handling, and mobile computing in their survey work as comprehensive security practices [36,37]. These security practices encompass a comprehensive list of the security practices that are most prone to security violations and compliance, and represent all sections of an information security policy that are essential to safeguard the confidentiality, integrity, and availability of information [88, 61]. These security practices were compiled from the Human Aspect of Information Security Questionnaire (HAIS-Q) and from security standards and policies [61]. Other security practices were identified in previous studies [47, 25], but the security practices in these studies are less comprehensive as compared to the HAIS-Q. Prior to usage, the HAIS-Q must always be updated to reflect current information security standards and policies [75].

12.1.3 Security practices

As outlined in the HAIS-Q, health care professionals' security practices include the security measures being adopted in the information security usage activities in response to security policies to safeguard the confidentiality, integrity, and availability of health care information systems. The requirements for such practices are usually expressed in regulations, directives, legislations, and security policies and specified in standards, best practices, and codes of conduct. Health care professionals' security practices include security measures being adopted in the usage of the internet, email, and social media, password management, incident reporting, information handling, and mobile computing [29], as required by information security policies and standards. For instance, in password management, how do users respond to periodic password changes as required by some security policies? When modeling human behavior with these theories, the independent variables (eg, professionals' associated characteristics or constructs shown in Table 12.1 and Figure 12.1) are often explored with the mediating variables (Figure 12.1), such as the professionals' security practices[85, 33]. Therefore, comprehensive security practices are needed to address those aspects most

prone to security violations, to ensure compliance, and to represent all sections of an information security policy that are essential for safeguarding the confidentiality, integrity, and availability of health care resources [86].

Table 12.1: Psychological, social-cultural, and demographic constructs

Construct	Definition, hypothesis, and the effect on security practice
Social demographics	Social demographics refer to professionals' demographics and work-related factors that influence their security practices [19]. Gender, workload, work emergency, role, department, and awareness or experience in information security all influence professionals' security practices. During health care emergencies or some health care scenarios, health care professionals behave contrary to established security policies if the security measures obstruct health care or threaten patient privacy. Such behaviors adversely impact security [47]. Individual differences also influence security practices [7].
Psychological characteristics	Psychological characteristics in this study refer to an individual's traits, perceptions, beliefs, thought processes, etc. These characteristics are influenced by various factors, including environmental factors [50]. Perceived severity of threat, perceived susceptibility, perceived barriers, perceived self-efficacy, and cues to action, attitude or personality, and emotions are some of the psychological characteristics that influence health care professionals' security practices. If health care professionals increase their awareness of the adverse impact on security, they tend to behave more consciously [67, 7].
Social factors	Social factors refer to the influence of peers and other professional groups. Social bonding, peer pressure, and trust level impact health care professionals' security practices [4,22]. Due to trust and social bonding among health care professionals, conscious care behaviors tend to be adversely affected among them [13, 14].
Cultural characteristics	Environmental norms, cultural beliefs, and assumptions impact security practices[88, 50]. This study mainly focuses on organizational culture and excludes the potential effect of national cultures. However individuals' cultural backgrounds also impact security-related behavior [62, 61, 1, 2].

12.1.4 Related Frameworks

In contributing to security conscious care behavior among health care workers, Humaidi et al [40] developed a conceptual framework for determining the statistical significance of perceptions. The study focused on security awareness and security technology related to health care professionals' security conscious behaviors. Protection motivation theory (PMT) and health belief model attributes were used as independent variables to determine their impact on security awareness and security technology mediat-

ing variables. Similarly, Cannoy et al employed the technology acceptance model (TAM), the theory of reasoned action (TRA), information assurance and security ethical behavior, organizational culture, and health information management [16] to develop a related framework. In the same context, Fernandez-Aleman et al advocated for more security awareness training to enhance good security practices and called for preventive and corrective actions to curtail incidents attributed to health care professionals [26]. The researchers studied the PSC context and some social demographic characteristics (age, gender, and experience). The security practices included password management, unauthorized accesses, disposal of sensitive information, and incidence reporting. The findings of the research provided some knowledge on the security gap between health care professionals' required and actual information security practices. Furthermore, the PMT and theory of planned behavior (TPB) [67] were adopted in a study to determine whether information security awareness, information security policy, and experience ultimately impact employee security practices. TPB relies on attitudes, subjective norms, and perceived behaviors to predict human behavior [3, 4]. The PMT deals with the ability to protect oneself from threats based on perceived severity of a threat, perceived probability of occurrence or vulnerability, the impact of the recommended preventive practices, and perceived self-efficacy [67]. Additionally, Hassan et al proposed a conceptual model for determining the drivers of information security culture in the health care context [36]. Secondary data were explored for the framework, and the researchers proposed that information security culture is influenced by behavioral change management, information security awareness, security requirements, and organizational systems and knowledge. Relatedly, Box et al reviewed the literature and proposed a model for information security compliant security practices within health care environments [14]. The researchers aimed to provide an overview of factors that were influencing or discouraging information security compliance. The constructs used in the model included compliance-promoting and misuse-deterrence factors, body of knowledge, attitudes, skills, behavioral interventions, and security compliant behavior. In an effort to improve health care professionals' conscious care behavior, van Deursen et al aimed to understand the sociotechnical risks of information security in the health care sector [80]. The study excluded the technical aspects of information security risks but focused on information security risks related to human and organizational factors. The researchers explored security incidents recorded in a central database by the Freedom of Information officers of the Scottish Health Boards and English Care Trusts. Various theories are used to model and assess the security practice of users. Lebek et al identified such theories, including the TRA/TPB, general deterrence theory, PMT, and TAM, as the most widely used theories for studying human security practices in the psycho-socio-cultural context

[18]. The systematic review by Lebek et al provided knowledge in common theories, but guidelines were not provided on the selection and application of these theories. Similarly, Yeng et al surveyed for related theories, security practices, and evaluation methods[88]. They found various theories that can be employed in modeling and analyzing health care security practice, as shown in Multimedia Appendix 18.7, Table 12.7; however, the approach was less systematic and lacks a framework. Health care security practices are not only impacted by social demographic traits (eg, age, gender, and experience) [86, 28, 43] or psychological traits, but also potentially influenced by other critical factors, such as emergency situations or workload as shown in Figure 12.1.

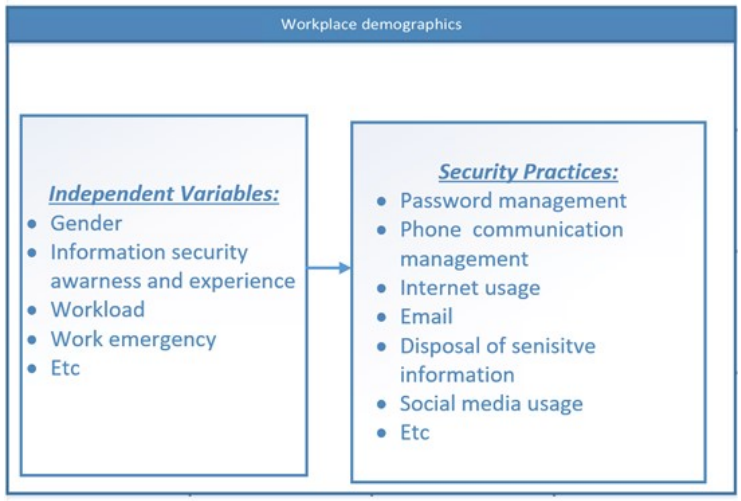


Figure 12.1: Relating independent variables with security practice

In view of the shortfall of the above framework to allow for the efficient study of health care professionals' security practices, we proposed the PSC framework to create a holistic set of healthcare professionals' characteristics for analyzing a wide range of security practices.

12.1.5 Problem Specification, Scope, and Contribution of the Study

Information security issues attributed to the human element have been recognized to be as important as technological security measures. Therefore, various frameworks have been developed in the psycho-socio-cultural context, but none is comprehensive within this study scope. Some of the frameworks were developed to assess only perception variables [88, 33, 18, 2, 75,

25]. Other frameworks adopted only social constructs [88, 16, 61, 3, 4] or cultural factors [18, 56, 41]. However, in a scenario where a study must be conducted with the aim of comprehensively understanding and addressing the information security challenges often faced by health care professionals, it is important to know which of the existing frameworks will be adequate. The reviewed frameworks [47, 67, 13, 14, 40, 7, 26, 36, 80, 41, 5, 73, 72, 79, 71, 59, 83, 84, 37, 68, 31, 38, 8, 60, 23, 27, 58] were not fully comprehensive. Meanwhile, security issues are affected by all these aspects and not just psychological, social, cultural, or sociodemographic aspects alone [7]. Therefore, a framework that can include all these aspects (Multimedia Appendix 18.7, Table 12.7) will be a comprehensive one. Furthermore, it is necessary to systematically structure the knowledge in a way that explicitly shows the connection between concepts in the study domain by using appropriate methods such as a domain ontology. The contribution of this study is a proposed holistic framework that consists of psychological, sociodemographic, and sociocultural variables, which can be used to analyze a comprehensive set of health care professionals' security practices, as shown in Table 12.1. The framework builds on studies collected in the literature review, as shown in Multimedia Appendix 18.8, Table 12.8. In order to comprehensively and explicitly represent the domain of interest, we also produced a domain ontology for developing the PSC framework. The purpose of the ontology is to enable the creation of a common understanding among people or software agents within a domain to share, reuse, and analyze domain knowledge [57, 34]. The security issues in health care organizations are not only attributed to health care workers' behaviors, but also stem from security awareness and organizational factors, such as IT competence of business managers, environment uncertainty, industry type, organizational preparedness, organizational culture, top management support, and organizational size. Various studies identified that organizational factors, including organizational size and industry type, have strong influences on IT [19, 44, 6] and implementation of information security management [17]. Notwithstanding, the scope of this study does not cover all organizational factors, but considers organizational factors and top management, with much focus on security issues directly involving health care workers, such as healthcare professionals who provide therapeutic measures (doctors, nurses, pharmacies, laboratory personnel, radiology officers, etc), IT personnel, health administrators, and finance personnel. The next section outlines the methods used in this study.

12.2 Method

12.2.1 General approach

We conducted a literature review of the state-of-the-art theories and security practices in health care in order to develop a holistic framework. According to previous reports [46, 12, 45, 63], there are various types of systematic studies. These include systematic mapping studies and systematic literature reviews. Systematic mapping studies perform reviews of topics in a broader sense by categorizing basic research articles into specific areas of interest. Systematic mapping studies have general research questions aimed at determining research trends or the state-of-the-art studies. Systematic literature reviews aim to aggregate evidence and therefore has a relatively specific research goal. To this end, a systematic mapping study was adopted in this work [46, 12] . Based on a review, we built and used an ontology to develop the PSC framework, which covers most of the dimensions of health care professionals' security-related traits. This framework allows for holistically analyzing health care security practices. The literature search was conducted between June 2019 and December 2019 through Google Scholar, Science Direct, Elsevier, IEEE Explore, ACM Digital, PubMed, and Scopus. Different keywords, such as "healthcare," "health," "staff," "employee," "professional," "information security," "behavior," and "practice" were used. To ensure a good-quality search strategy, the keywords were combined using the Boolean functions "AND," "OR," and "NOT." Peer-reviewed journals and articles were considered. The inclusion and exclusion criteria were developed based on the study objective and through discussions among the authors. Initially, 337 articles were selected by skimming through the titles and keywords for articles that aligned with the inclusion and exclusion criteria. Screening was further applied by quickly reading the abstracts and keywords. Duplicates were then filtered out, and articles that appeared relevant, based on the inclusion and exclusion criteria, were read in their entirety and evaluated. Twenty-six articles were further removed from the study in the full reading and evaluation stage based on various reasons, including limited scope and articles not meeting the inclusion and exclusion criteria. For instance, a study [52] looked into security issues in health care using a machine learning approach, but this was out of the scope of this study. Furthermore, another study looked [54] into an assessment model for software quality issues in health care, but security was not the main focus. Based on these and other similar reasons, the number of articles that were included in the study reduced greatly. Other relevant articles were also retrieved through the reference lists found in the literature. Figure 12.2 presents a Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) flow diagram that clarifies article selection and screening [66].

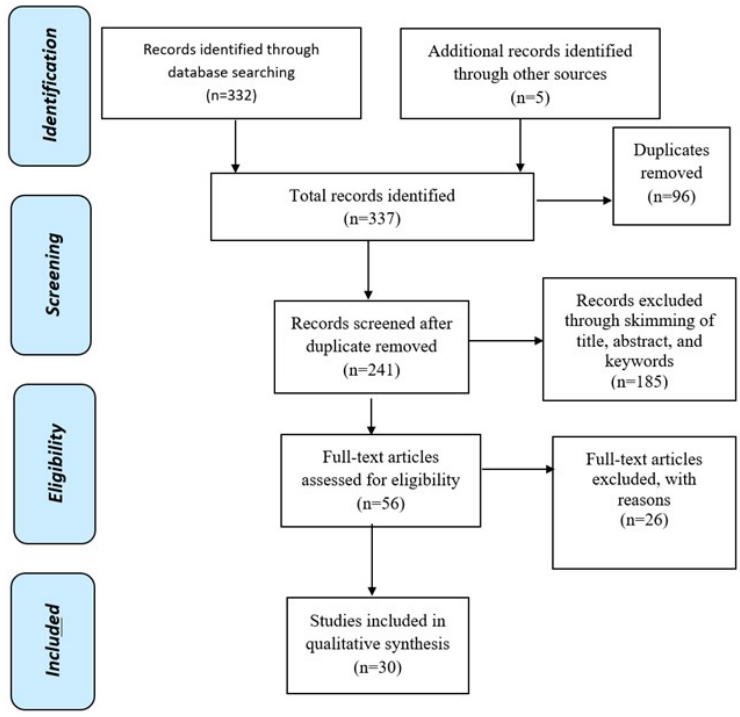


Figure 12.2: Presentation of reviewed articles on PRISMA diagram

12.2.2 Inclusion and Exclusion Criteria

Articles included in the review were required to be about security practices in the health care context and to pertain to health care professionals' information security behavior in relation to their work. Other articles, such as those that were not related to the health care context and did not focus on human behavior in health care, were excluded.

12.2.3 Data Collection and Categorization

Data collection and categorization were established from the study objective through completion of the literature review and based on discussions of the authors. In order to assess, analyze, and evaluate the study, these categories were exclusively defined as follows: (1) Theory used: This category includes only theories (psychological, social, or cultural theories) used in the study to relate human characteristics to the security practices. (2) Security practice: This category includes the security measures (eg, password management, incident reporting, and internet usage) used in the study. (3) Study type:

This category specifies the type of study, whether theoretical or empirical. In this study, "empirical" refers to practical studies conducted in health care contexts and "theoretical" refers to reviews and proposed frameworks for related studies. (4) Study context: This category specifies what area (eg, psychological, social, cultural, or demographic context) the study covered. Multimedia Appendix **??**, 12.8 presents the categorization of the included literature.

12.2.4 Literature Evaluation and Analysis

The selected articles were assessed, analyzed, and evaluated based on the above defined categories. We performed an analysis on each of the categories (theory used, security practice, study type, and study construct) to evaluate the state-of-the-art approaches. The percentages of the attributes for the categories were calculated based on the total number of counts (n) of each attribute type. Some studies used multiple categories; therefore, the number of counts for these categories exceeded the total number of articles presented in the study.

12.3 Literature Review Findings, Ontology, and PSC Framework

This section presents the findings of the literature review, the ontology, and the proposed theoretical framework. The searches in the aforementioned online databases resulted in a total of 337 records being initially identified by following the guidelines of the inclusion and exclusion criteria in the reading of titles, abstracts, and keywords. We further screened and selected articles by reading the objective, method, and conclusion sections of each study, and this led to a further exclusion of 185 articles that did not meet the defined inclusion criteria. A total of 96 duplicates were also removed, and the remaining 56 articles were fully read and appraised. After the full-text reading, a total of 30 articles were included and analyzed in the study (Figure 12.2). Table 12.2 presents the theories identified in the literature review. The theories that were most often used in analyzing the security practices of health care professionals included the health belief model (21%), TPB (18%), general deterrence theory (14%), PMT (14%), and technology acceptance theory (7%), as shown in Table 12.2.

12.4 Proposed Ontology

Ontologies are formal specifications of key concepts within a domain and the relationships among them. Ontologies are purposeful artefacts that make

Table 12.2: Psychological, social, and cultural theories

Theory	Count(N)
Health belief model [41]	6
Theory of planned behavior [67]	5
General deterrence theory [79]	4
Protection motivation theory [67]	4
Technology acceptance theory[88]	2
Technology threat avoidance theory [68]	1
Social bond theory [82]	1
Situational crime prevention cite54theoharidou2005insider	1
Institutional theory [8]	1
Grounded theory [27]	1
Social control [16]	1
The big five theory [16]	1

Table 12.3: Security practices.

Security practice	Count (N)
Password management [26, 80, 73]	6
Security policy and procedure [31]	3
Unauthorized Disclosure [31]	3
Email use with sensitive data [88]	2
Logging off session [88, 5]	2
Emergency access[88]	2

Table 12.4: Categories of the studies identified

Category	Count	%
Psychology	7	35
Demographics	6	30
Social	3	15
Cultural	3	15
Linguistics	1	5

domain assumptions explicit, enable the construction of a common understanding among stakeholders, enable the reuse of expert knowledge, etc [73]. The proposed ontology contained a total of eight distinct concepts and nine relationships, which enabled us to capture the conceptual relationship between a total of 76 unique instances extracted from the literature. Figure 12.3 presents the ontology capturing key concepts of the HSPAMI project and the supporting empirical evidence that corresponds to the PSC frame-

work. The relationships among concepts are represented by the arrows between concepts in the rectangles. The following subsections describe the steps followed for the construction of the ontology based on the guidelines presented in a previous report [57].

12.4.1 Development of the Ontology

The main objective of the proposed ontology was to map the HSPAMI main study areas to empirically supported research results in order to develop a literature-based comprehensive holistic framework that can be utilized in the project and by researchers or practitioners interested in the domain of information security within the health care context [88]. Determine the Domain and Scope of the Ontology The proposed ontology aimed to (1) structure the main focus areas of the HSPAMI project, (2) create a connection between these study areas and existing empirical research results, and (3) develop a comprehensive PSC framework that efficiently communicates domain knowledge to various stakeholders. Thus, the domain is defined as health care professionals' security practices, and the scope is restricted to research results investigating the relationship between psychological and sociocultural theories and variables with respect to security behaviors.

12.4.2 Use of Existing Ontologies

Literature searches were conducted for existing comprehensive domain ontologies on Google Scholar, ScienceDirect, and Scopus, with the following keywords: "ontology," "healthcare," "security behavior," and "practice." These keywords were also combined with the Boolean functions of "AND," "OR," and "NOT." No comprehensive ontology was identified. Ontologies that explicitly model and structure the domain have been proposed for various purposes in the health care domain, such as interoperability [9] regulating access control for internet of things–based health care [2, 39]. The ontology proposed in this paper uses the HSPAMI study areas as an organizing principle for the existing empirically supported research results [2, 39].

12.4.3 List of the Relevant Terms of the Domain

The fundamental concepts were identified in a previous report [4] with respect to the main study areas of the HSPAMI project. These are health care professionals' psychosocial and cultural demographic variables, security practices, and the incentivization of security practices. The concepts were aligned with the classes commonly encountered in empirical studies investigating the relationship between theoretical constructs and behaviors of interest or outcome variables (eg, security practices).

12.4.4 Define the Classes and the Class Hierarchy

In order to represent the relationship between concepts of the domain and empirical research results, the classes were conceptually connected to each other. The combination approach was followed in defining the classes and hierarchy, which combined top-down and bottom-up approaches. More salient concepts (HSPAMI concepts and study components) were defined first, and then, based on the identified empirical results, more specific concepts were included. To deal with different terminologies applied to similar concepts (synonyms), the equivalence of classes is represented by the "isEquivalentTo" relationship between concepts, which is inherited by the instances added to the classes. Thus, theories that consist of constructs can be included in the ontology by defining and connecting an instance to the accompanying theory. Variables that are not specifically part of any theory (eg, demographic variables) can be included by restricting the domain attribute to the class of constructs. Table 12.6 shows the existing classes defined within the ontology, with example instances. Based on the literature review, a total of eight classes have been defined as the most general concepts, as shown in Figure 12.3.

Table 12.5: Main concepts defined as classes.

Classes	Instances
Healthcare security practice analysis, modeling and incentivization (HSPAMI)	-
HealthCareStaff	Doctors, nurses, etc
Intervention/Incentivization	Motivation, deterrence, etc
PsychoSocialCulturalDemographicVariable	Gender, age, etc
SecurityPractice	PasswordManagement, EmailUse, etc
Theory	Theory of planned behavior, protection motivation theory, etc
Construct/IndependentVariable	Attitude, SubjectiveNorm, etc

12.4.5 Define Properties of Classes

The main objective of this step was to describe the relationship of a class to other individuals. The properties were defined at the most general class; thus, all members of that class inherited the given property. Table 12.7 shows the relationships and the connected classes in the proposed ontology. A total of nine properties link various concepts in the ontology.

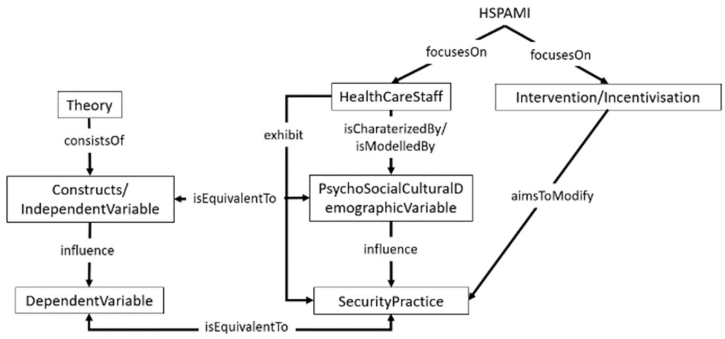


Figure 12.3: Structure of the ontology representing the concepts as classes and specifying the relationships among the classes

Table 12.6: Relation of classes

Relation of classes	Classes connected
consistsOf	Theory - Construct
influence	IndependentVariable - DependentVariable
isEquivalentTo	Construct - PsychoSocialCulturalDemographicVariable
exhibit	HealthCareStaff - SecurityPractice, DependentVariable
isCharacterizedBy/isModeledBy	HealthCareStaff - Construct
aimsToModify	Intervention/Incentivization - SecurityPractice
focusesOn	HSPAMIa - Intervention, HealthCareStaff
isATypeOf	Gender - Construct
hasAttribute	SelfEfficacy - Psychological; Gender - Demographic

12.4.6 Define the Data-Type Properties

This step was excluded in the development of the ontology at this stage. Since ontologies can be developed at various levels of granularity, these steps may be iteratively completed at a future stage when the requirements (eg, development of software) are defined more specifically. For the purpose of creating a comprehensive framework of health care staff characteristics and security practices, this step was unnecessary.

12.4.7 Create Instances

The research papers meeting the inclusion criteria were subsequently analyzed in detail to extract the instances for the previously enumerated classes. The list of papers reviewed for constructing the ontology are presented in multimedia Appendix 12.8, Table 12.9.

For the purpose of demonstration, Figure 12.4 and Figure 12.5 present how instances can be included in the existing ontology. Additional properties (eg, equivalence of classes) can be represented, which is especially important to avoid ambiguity and for clarifying the semantic meaning of different concepts when they are related (eg, self-efficacy is equivalent to perceived behavioral control). Each theory discussed in a previous report [83] is represented as an instance of the theory class, and the object property "isATypeOf" is proposed to capture the relationship. The TPB consists of the following three constructs: "AttitudeTowardBehavior," "SubjectiveNorm," and "PerceivedBehavioralControl," which is equivalent to beliefs related to self-efficacy.

12.4.8 Ontology and the PSC Framework

The framework shown in Figure 12.6 consists of independent variables, mediating variables, and the dependent or target variable. The independent variables have various constructs, including psychological traits, social factors, cultural influences, and sociodemographic characteristics. Attributes of these constructs were associated with comprehensive security practices. The security practices serve as the mediating variables. The target or dependent variable, known as health care professionals' security metrics, was obtained after relating the independent and mediating variables. The framework components are as follows:

(1) Independent variables: This aspect of the PSC framework consists of the characteristics of the health care staff that can impact health care professionals' security practices. With reference to Figure 12.4 and Figure 12.6, these characteristics are segregated into psychological or perception variables, sociodemographics, and social and cultural attributes. The psychological traits include perception variables or constructs, such as perceived severity, perceived susceptibility, perceived cues to action, perceived barriers, and perceived self-efficacy, personality, and emotions.

(2) Social bonding: Social bonding is related to social behaviors that can influence health care personnel's information security behavior. Such constructs include social bonding, peer pressure, and trust level, as shown in Figure 12.6.

(3) Cultural factors: Culture-related traits that can impact information security include environmental norms, beliefs, and assumptions. (4) Social demographics: Social demographics, such as gender, workload, information

security experience, emergency, role, and experience, are hypothesized to have an impact on information security relating to health care staff.

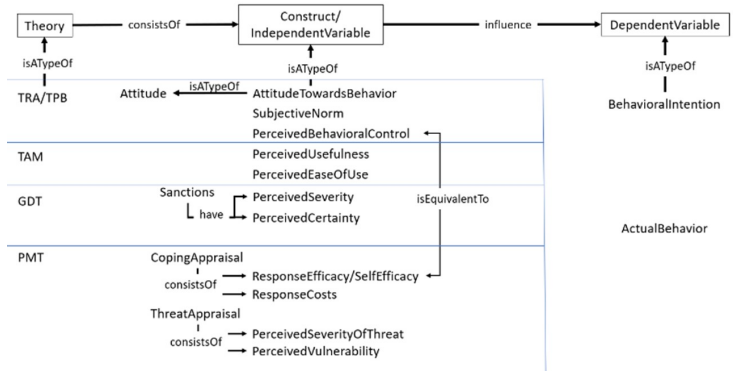


Figure 12.4: Instances and additional properties defined from the review paper

Figure 12.4 presents the expansion of the ontology with empirical results that have particular theories associated with them. Psychological, cultural, and demographic variables were grouped by defining additional attributes to facilitate knowledge sharing.

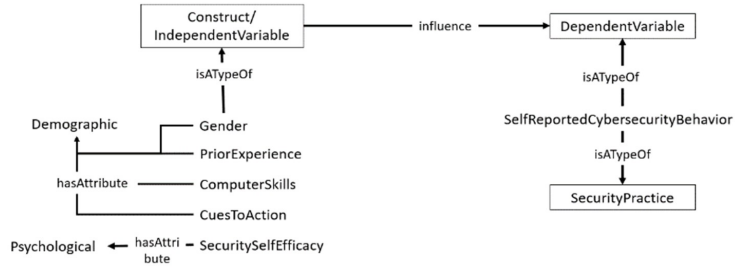


Figure 12.5: Expansion of the ontology based on results from [7]

The PSC framework also has mediating variables that are basically the security practices of the health care staff. The health care security practices are the required security-related behaviors defined in the policies, standards, regulations, and codes of conduct for health care personnel. Health care staff are therefore required to abide by such security measures to enhance the confidentiality, integrity, and availability of health care data. The security practices in the PSC framework were adopted from the HAIS-Q. The HAIS-Q is a framework consisting of a comprehensive information security practice. In a typical health care environment, health care staff mem-

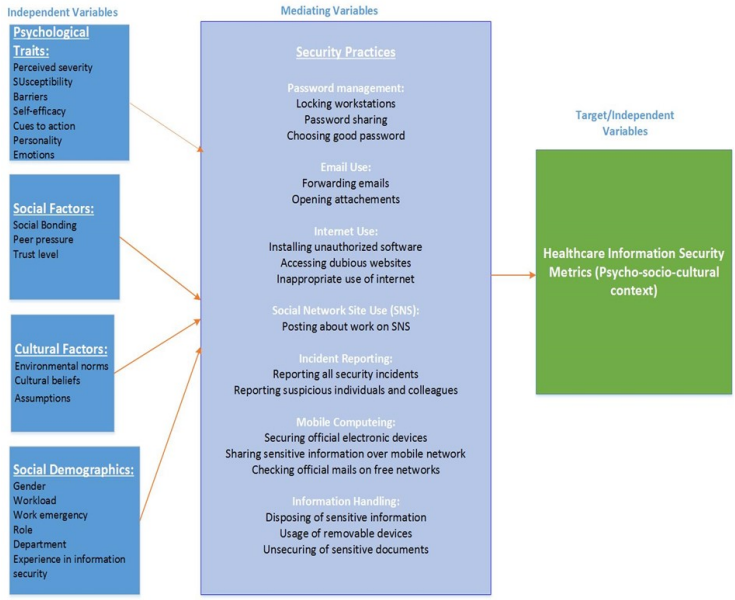


Figure 12.6: Proposed PSC framework

bers go through their daily security practices within the scope of the HAIS-Q, and these security practices are impacted by independent variables. Security practices include social network usage, password management, incident reporting, mobile computing, and internet use, as shown in Figure 12.6.

Finally, the target or the dependent variable is the measured security practice of the health care staff. Such a security metric can therefore be used for management decision-making, such as implementing intervention measures aimed to improve conscious care security practices.

12.5 Discussion

12.5.1 Principal Findings

Information security management for mitigating data breaches involves identifying the threats to information security and devising efficient countermeasures [30]. Information security management includes adding tools and serving employees with checklists of information security user policies for work roles, as well as requiring employees to abide by those policies. However, the security of health care data also requires systematic analysis of the health care professionals' security practices for building a "human firewall,"

with the objective of enhancing a conscious care and security resilience culture. Thus, identification of various sources of human threats in the social, cultural, and psychological contexts is vital [87, 62, 61, 1]. To this end, we identified constructs capturing the psychological, sociocultural, and demographic variables (termed in this study as "psychosociocultural context") to develop the PSC framework to understand health care professionals' security practices. The main contribution of this paper is the development of the PSC framework implemented as a domain ontology. Specifically, the framework includes concepts and important variables that have been empirically proven to influence the behavior (ie, security-related practices) of health care professionals when dealing with sensitive information in a health care work setting. Based on the overview of existing literature [47, 67, 13, 14, 40, 7, 26, 36, 80, 41, 5, 73, 72, 79, 71, 59, 83, 84, 37, 68, 31, 38, 8, 60, 23, 27, 58], we concluded that existing frameworks lack a comprehensive and holistic perspective. Furthermore,[67, 80, 41, 72, 59, 84, 37, 68] not all frameworks provide strong empirical support for the inclusion of variables from the perspective of both security related-behaviors and professionals' characteristics. Therefore, this paper represents a step toward creating a comprehensive and practically useful framework that can aid information security practitioners in fulfilling their work requirements by incorporating the relevant concepts and research results that serve as a foundation of the framework.

The utility of the proposed framework will be tested in the HSPAMI project by scoping the forthcoming investigations on factors that must be considered in monitoring and modifying health care professionals' security-related behaviors. While specific empirical research papers are necessarily limited with respect to their scope on the security practices and the theories utilized, such papers provide the crucial building blocks of the overarching framework. The first major advantage of the present framework is that it encompasses accumulated knowledge by utilizing the evidence from previous investigations (each focusing on narrowly defined behaviors [47, 18, 7, 61, 56, 48, 10, 51], eg, responding to spam and sharing information on social media); thus, the frame

work provides a more comprehensive perspective on the various forms of security-related behaviors that should be investigated. This aspect of the present framework is mainly supported by the inclusion of the concepts found in the HAIS-Q instrument, which is a validated and widely utilized questionnaire for measuring information security–related beliefs, knowledges, and attitudes [62, 61, 1].

Based on the literature survey, we also developed an ontology to include significant concepts for the development of the PSC framework. Within the PSC context of health care professionals' security practices, various studies exist [67, 40, 26]. The second major contribution therefore involves the selection of psychological, social, and demographic variables (ie, constructs

and theories) from existing literature [47, 18, 7, 61, 80, 56, 48, 10, 51] and the representation of the framework in the form of a domain ontology. By specifying the framework as an ontology, we efficiently structure, organize, and reuse the vast amount of existing knowledge. Furthermore, the ontology also enables an efficient way to share information with other stakeholders within and outside the HSPAMI project without ambiguities, thus helping to build a common understanding. This aspect is exemplified by object relations that link synonyms or different terminologies used for the same construct to build a common language shared by all stakeholders involved in project-related activities. Finally, the ontology may as well serve as a blueprint for applications developed within the project, such as relational databases containing the relevant variables and specifying the connections between them.

Evaluation of the ontology refers to judgments about the technical features of the ontology and assessment of its usability and utility. Generally, evaluation aims at ensuring the correctness and completeness of an ontology [32]. It is an iterative process, which can be conducted at each point of the ontology's life cycle. An evaluation must be done against a frame of reference, which may be a set of competency questions and requirements, and the real world [32] and may take the form of a technical evaluation in the lab or at the location of application (eg, health care context with health care professionals). Evaluation may be performed with several criteria as follows: evaluation of definitions (checking for the absence of well-defined properties in the ontology), structure of the ontology (matching the ontology's structure with the design criteria of the environment, where it is intended to be used), syntax of definitions (ensuring that syntactically correct keywords are present), content of definitions (identify what concepts are covered, what concepts are not included, or included incorrectly), consistency (avoidance of contradictions), completeness (extent of covered concepts in the domain of interest), and conciseness (check whether information contained in the ontology is relevant and accurate) [32]. As the ontology has been developed using existing empirical research results, its validity partially depends on the reliability and validity of the findings in the knowledge base. Furthermore, at this stage of development, only a technical evaluation is possible, thus its validation in real-world settings is among the key goals of future work. Eventually, the practical benefits of the ontology depend on its recognition and approval among experts who utilize it [15].

With respect to the comprehensiveness of the current PSC framework, it is comparable to similar approaches [8,32] with a stronger focus on the requirement that only empirically supported research results should be included. While this may limit the comprehensiveness of the framework, it ensures that only relevant and practically significant theories and concepts are investigated and applied during the activities of the overall project, which

can save time and other valuable resources during the process. The real-world evaluation of the framework in terms of its usefulness for sharing and analyzing knowledge, creating a common understanding, and representing concrete aspects of the envisaged application domain will be studied within the scope of the project through case studies, field experiments, or other research methods. To complement the efforts of health care professionals in maintaining the confidentiality, integrity, and availability of health care data, a systematic approach to identify the detailed and subtle health care professionals' characteristics that impact information security practices must be applied. All these constructs are vital when measuring the conscious care behavior of health care professionals. For example, if we assume that psychological constructs are not measured in a typical empirical study of security conscious care behavior, there will be a gap since the perception of the health care security practice will not be captured [87]. Thus, if security solutions are professed based on such a study, the solutions will lack measures to deal with the perception aspect.

Therefore, through the PSC framework developed in this paper, we have identified various constructs within the project domain. The holistic approach is much needed because it strives to capture the entire problem area in the scope of the project. Focusing on just one or two aspects of staff-related traits that impact security in the health care industry might not be sufficiently effective [87] For instance, some of the frameworks focused only on social factors, with the exclusion of other factors, such as the perception. Without determining how health care staff perceived the severity of the impact of their information security malpractices in a related study, health care professionals may not be treated with appropriate incentivization methods for improving such malpractices. Lack of perception variables implies that health care staff would not be able to perceive the gravity of their security-related malpractices, which means there may still be data breaches resulting from untreated psychological traits. Conversely, if a study is conducted with only psychological constructs, data breaches may still occur as a result of untreated social-related constructs, such as social bonding and peer pressure. An approach, such as the PSC framework, therefore appears necessary for an efficient study.

12.5.2 Conclusion and Future Work

The mutual trust between health care professionals and their patients is under threat owing to frequent and large data breaches in health care. Furthermore, the richness of the health care data is attracting cyber criminals. Since scaling universal technological security measures is challenging, cyber criminals tend to exploit the health care staff for easy entry. To curtail this ascendance in data breaches, a comprehensive set of health care professionals' characteristics and security practices, which can impact information

security, was identified. An ontology was developed from the identified literature generated by a literature review. Then, a holistic PSC framework was developed. The framework can be implemented with a mixed method approach encompassing both qualitative and quantitative studies [80, 55].

Owing to the systematic approach used to develop the PSC framework, it is possible to identify reliable security metrics while considering all the subtle personnel characteristics of health care professional and their related security practices. Such metrics can then be used to develop incentivization or motivational measures aimed toward building stronger "human firewalls" to curtail data breaches in health care. Beyond the conventional qualitative evaluation methods of interviews and questionnaires or surveys, other approaches, including team-based learning [88] and the Delphi method [46], should be explored in the future to enrich empirical studies using comprehensive frameworks such as our PSC framework. Additionally, organizational factors should be considered in the future, since they were not entirely covered in this study.

Furthermore, clarifying the meaning and interconnectedness of various terms imported from different domains (eg, psychology, information security, sociology, etc) can be beneficial for discovering contradictory or converging pieces of evidence revealed by researchers. While the ontology currently captures only a limited number of concepts from the PSC and demographic contexts of health care professionals, it is flexible and can be extended with new results based on advances in the literature. The level of granularity can, for instance, be increased depending on the requirements of the applications in future work. The emphasis on the empirical foundations could also be strengthened by representing associations between variables through specifying additional object properties associated with the classes (eg, correlations, predictive accuracy, etc). The compatibility of this domain ontology with other ontologies (eg, health care staff demographic characteristics in employee databases) needs to be investigated in future work to increase reusability and to achieve a more realistic mapping between research results and the opportunities to observe the variables included in the framework. Additional expert knowledge could also be useful for enriching the framework, which can be achieved through iterative workshop sessions with other stakeholders (eg, health care staff, security practitioners, etc).

12.6 Multimedia Appendix 1

12.7 Multimedia Appendix 2

12.8 Multimedia Appendix 3

Table 12.7: Analysis of the theories and their application areas in the Healthcare Security Practice Analysis Modeling and Incentivization (HSPAMI)

HSPAMI study area	Theories that support study area
Social Bonding (SB)	SC [18]
Peer Pressure (PP)	SC[18]
Social Norms and Beliefs (SNB)	SC, HBM[18, 56]
Healthcare Emergency (HCE)	PMT, SC, TPB [67, 18, 48]
Work Load (WKL)	PMT, HBM [56, 48]
Privacy and Security perception	PMT, DT, HBM [18, 56, 48]
Personality and Attitude (PA)	TBF, TPB, HBM [47, 13, 70]
IS Experience, Education and Knowledge (IEEK)	PMT [13]
Emotions	PMT, HBM [67, 56]

12.9 Bibliography

[1] A., C. . hais-q: A smart solution to cyber security., 2017. Available from: `https://www.dst.defence.gov.au/podcast/hais-q-smart-solution-cyber-security`. 333, 347

[2] AGRAWAL, V. Towards the ontology of iso/iec 27005: 2011 risk management standard. In *HAISA* (2016), pp. 101–111. 333, 336, 341

[3] AJZEN, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of applied social psychology 32*, 4 (2002), 665–683. 334, 336

[4] AJZEN, I., AND MADDEN, T. J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology 22*, 5 (1986), 453–474. 334, 336

[5] ALBARRAK, A. I. Evaluation of users information security practices at king saud university hospitals. *Global Business & Management Research 3*, 1 (2011). 336, 340, 347, 352

[6] ALSHAWAF, A. H., ALI, J. M., AND HASAN, M. H. A benchmarking framework for information systems management issues in kuwait. *Benchmarking: An International Journal* (2005). 336

Table 12.8: Theories used in the study

	Ref.	Theory Used	Security Practice	Context Used	Study Type (E= "empirical study" T= theoretical study")
1	[67]	The protection motivation theory and theory of planned behavior (TPB)	Information security awareness, security policies and procedures, security experience	Psychological, demographic	E
2	[41]	Health belief model (HBM)	Security, awareness user's health, information system's security compliance behavior	Psychological, demographic	E
3	[68]	Technology threats avoidance theory		Psychological, demographic (gender, age, and position)	E
4	[37]	Organizational culture characteristics and health belief model (HBM)		Culture	E
5	[84]		Security education, security technology investment		E
6	[83]			Culture	T
7	[13]	Literature review, coping model of user adaptation and framework for classifying emotions as a tool			T
8	[14]	Literature review			T
9	[80]	Delphi study	Staff leaving data assets unattended on the premises, and these assets consequently go missing; staff sharing passwords to access patient data; and staff sending email containing personal patient data to the wrong addressee, thus disclosing data to unauthorized persons		E
10	[59]	General deterrence theory	Discloser of sensitive information	Social	E
11	[71]		Adherence to organizational policy		T
12	[79]	General deterrence theory, social bond theory , social learning theory , theory of planned behavior (TPB), situational crime prevention		Social	T
13	[72]	"Health belief model (HBM), theory of planned behavior (TPB), and the health action process approach		Psychological	E
14	[73]			Demographic	T
15	[5]		Password management, logging off sessions		T
16	[31]		Security awareness, security policy, organizational culture, security culture		T
17	[40]	Protection motivation theory (PMT) and health belief model (HBM)		Psychological	T
18	[38]		Password management, unauthorized access		E
19	[8]	The institutional theory	Security policy		T
20	[60]		Self-efficacy to comply, patient's medical status		E
21	[26]		Password management, confidential information discarding, unauthorized access via computer screen, reporting security violations		E
22	[23]	Vocabulary test		Linguistic	E
23	[80]		Information security awareness, knowledge		T
24	[9]		Authentication, de-authentication, permission management		E
25	[27]	Grounded theory (GT)	Access control, access control policies, access in emergency situations, access control solutions		T
26	[58]		Authentication		E
27	[57]	Health belief model (HBM) (Rosenstock,1974) and protection motivation theory	Computer skills, experience with cyber security practice	Demographic, Psychological	E
28	[16]	Technology acceptance model (TAM)		Psychological	E
29	[10]	Theory of planned behavior (TPB), general deterrence theory			T
30	[88]	Health belief model (HBM), protection motivation theory (PMT), theory of planned behavior (TPB), the big five (TBF) model, and social control	Internet use, email use, social media use, password management, incident reporting, information handling, and mobile computing	Psychological, social, cultural, demographics	T

[7] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., AND XU, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. xv, 333, 336, 345, 347, 348, 353

Table 12.9: Articles used to construct the ontology.

TRA/TPB, TAM, GDT, PMT	Theory	
Attitude, Sanctions, CopingAppraisal, ThreatAppraisal, AttitudeTowardBehavior, SubjectiveNorm, PerceivedBehavioralControl, PerceivedUsefulness, PerceivedEaseOfUse, PerceivedSeverity, PerceivedCertainty, ResponseEfficacy, ResponseCost, SelfEfficacy, PerceivedSeverityOfThreat, PerceivedVulnerability, BehavioralIntention	Construct/IndependentVariable, PSC varialbe	[48]
ActualBehavior	DependentVariable, SecurityPractice	
Demographic, Gender, PriorExperience, ComputerSkills, CuesToAction, SecuritySelfEfficacy,	Construct/IndependentVariable, PSC varialbe	[7]
SelfReportedCybersecurityBehavior	DependentVariable, SecurityPractice	
HBM	Theory	[56]
PerceivedSuspectibility	Construct/ Independent Variable, PSC varialbe	
PerceivedBenefits		
SelfEfficacy		
EmailSecurity	DependentVariable, SecurityPractice	
Unattended asset goes missing, Password or access token sharing, Email to wrong recipient, Theft on premises, Procedure not followed, Wrong privileges set, High-impact mistakes, Working in public place, Unsecure remote third party, Transportation, Family breach, Backup medium goes missing, Improper disposal, Third-party discloses data, Unsecure remote working, Trainee breach, Patient breach, Covering up errors	DependentVariable, SecurityPractice	[80]
AttachmentToJob, AttachmentToOrganization, CoworkerBehavior, SubjectiveNorms, Commitment, PerceivedSeverity	Construct/IndependentVariable, PSC varialbe	[18]
BehavioralIntention,	DependentVariable, SecurityPractice	
PerceivedCertaintyOfSanction, PerceivedSeverityOfSanction, Attitude	Construct/IndependentVariable, PSC varialbe	[10]
BehavioralIntention	DependentVariable, SecurityPractice	
PasswordSharing, AutheticationCircumvention, DeAutheticationCircumvention, PermissionManagement, RepresentationBreaking	DependentVariable, SecurityPractice	[9]
Conscientiousness, Agreeableness, EmotionalStability, RiskTakingPropensity,	Construct/IndependentVariable, PSC varialbe	[51]
InformationSecurityAwareness	DependentVariable, SecurityPractice	
PasswordManagement, EmailUse, InternetUse, SocialMediaUse, MobileDeviceUse, InformationHandling, IncidentReporting	DependentVariable, SecurityPractice	[61]
**PsychoSocialCulturalDemographicVariable = "PSC varialbe"		

[8] APPARI, A., JOHNSON, M. E., AND ANTHONY, D. L. Hipaa compliance: an institutional theory perspective. 336, 340, 347, 352

[9] ASIM, M., PETKOVIĆ, M., QU, M., AND WANG, C. An interoperable security framework for connected healthcare. In *2011 IEEE Consumer Communications and Networking Conference (CCNC)* (2011), IEEE, pp. 116–120. 341

[10] AURIGEMMA, S., AND MATTSON, T. Do it or else! exploring the effectiveness of deterrence on employee compliance with information security policies. 347, 348, 352, 353

[11] AYYAGARI, R. An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security 8*, 2 (2012), 33–56. 330

[12] BOOTH, A., PAPAIOANNOU, D., AND SUTTON, A. Systematic approaches to a successful literature review: Sage publications, 2012. 337

[13] BOX, D., AND POTTAS, D. Improving information security behaviour in the healthcare context. *Procedia Technology 9* (2013), 1093–1103. 329, 330, 332, 333, 336, 347, 351, 352

[14] BOX, D., AND POTTAS, D. A model for information security compliant behaviour in the healthcare context. *Procedia Technology 16* (2014), 1462–1470. 329, 330, 333, 334, 336, 347, 352

[15] BUSSE, J., HUMM, B. G., LÜBBERT, C., MOELTER, F., REIBOLD, A., REWALD, M., SCHLÜTER, V., SEILER, B., TEGTMEIER, E., AND ZEH, T. Actually, what does "ontology" mean? *Journal of computing and information technology 23*, 1 (2015), 29–41. 348

[16] CANNOY, S. D., AND SALAM, A. F. A framework for health care information assurance policy and compliance. *Communications of the ACM 53*, 3 (2010), 126–131. 329, 334, 336, 340, 352

[17] CHANG, S. E., AND HO, C. B. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems* (2006). 336

[18] CHENG, L., LI, Y., LI, W., HOLM, E., AND ZHAI, Q. Understanding the violation of is security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security 39* (2013), 447–459. 331, 335, 336, 347, 348, 351, 353

[19] CHOU, H.-W., AND JOU, S.-B. Mis key issues in taiwan's enterprises. *International journal of information management 19*, 5 (1999), 369–387. 336

[20] CNN. A convicted hacker debunks some myths -, July 2015. Available from: `http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna`. 330

[21] CONNOLLY, L. Y., LANG, M., GATHEGI, J., AND TYGAR, D. J. Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security* (2017). 331

[22] DIGITALHEALTH. Norway healthcare cyber-attack could be biggest of its kind, July 2019. Available from: `https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/`. 328

[23] DREVIN, L., KRUGER, H., BELL, A.-M., AND STEYN, T. A linguistic approach to information security awareness education in a healthcare environment. In *IFIP World Conference on Information Security Education* (2017), Springer, pp. 87–97. 336, 347, 352

[24] DRYE CANNOY, S., AND SALAM, A. F. A framework for health care information assurance policy and compliance. *Communications of the ACM 53*, 3 (2010), 126–131. 329, 330

[25] EGELMAN, S., AND PEER, E. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (2015), pp. 2873–2882. 332, 336

[26] FERNÁNDEZ-ALEMÁN, J. L., SÁNCHEZ-HENAREJOS, A., TOVAL, A., SÁNCHEZ-GARCÍA, A. B., HERNÁNDEZ-HERNÁNDEZ, I., AND FERNANDEZ-LUQUE, L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics 84*, 6 (2015), 454–467. 334, 336, 340, 347, 352

[27] FERREIRA, A., ANTUNES, L., CHADWICK, D., AND CORREIA, R. Grounding information security in healthcare. *International Journal of Medical Informatics 79*, 4 (2010), 268–283. 336, 340, 347, 352

[28] FOR EHEALTH, D. Code of conduct for information security and data protection in the healthcare and care services sector, April 2019. Available from: `https://www.ehelse.no/normen/documents-in-english`. 335

[29] GDPR. Implementation of gdpr in health care sector in norway, 2019. Available from: `https://ehelse.no/personvern-og-informasjonssikkerhet/eus-personvernforordning/implementation-of-gdpr-in-health-care-sector-in-norway`. 330, 332

[30] GDPR. Key changes with the general data protection regulation, 2019. Available from: `:https://eugdpr.org/the-regulation`. 330, 346

[31] GEBRASILASE, T., AND LESSA, L. F. Information security culture in public hospitals: the case of hawassa referral hospital. *The African Journal of Information Systems 3*, 3 (2011), 1. 336, 340, 347, 352

[32] GÓMEZ-PÉREZ, A. Some ideas and examples to evaluate ontologies. In *Proceedings the 11th Conference on Artificial Intelligence for Applications* (1995), IEEE, pp. 299–305. 348

[33] GORDON, W. J., WRIGHT, A., AIYAGARI, R., CORBO, L., GLYNN, R. J., KADAKIA, J., KUFAHL, J., MAZZONE, C., NOGA, J., PARKULO, M., ET AL. Assessment of employee susceptibility to phishing attacks at us health care institutions. *JAMA network open 2*, 3 (2019), e190393–e190393. 330, 332, 336

[34] G'ABOR, N., ET AL. Ontology development, in semantic web services: Concepts, technologies, and applications,, 2007. 336

[35] HARTVIGSEN, G., AND PEDERSEN, S. Lessons learned from 25 years with telemedicine in northern norway, 2015. 329

[36] HASSAN, N. H., AND ISMAIL, Z. A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia-Social and Behavioral Sciences 65* (2012), 1007–1012. 334, 336, 347

[37] HASSAN, N. H., MAAROP, N., ISMAIL, Z., AND ABIDIN, W. Z. Information security culture in health informatics environment: A qualitative approach. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (2017), IEEE, pp. 1–6. 336, 347, 352

[38] HEDSTRÖM, K., KOLKOWSKA, E., KARLSSON, F., AND ALLEN, J. P. Value conflicts for information security management. *The Journal of Strategic Information Systems 20*, 4 (2011), 373–384. 336, 347, 352

[39] HENRIQUES, G., LAMANNA, L., KOTOWSKI, D., HLOMANI, H., STACEY, D., BAKER, P., AND HARPER, S. An ontology-driven approach to mobile data collection applications for the healthcare industry. *Network Modeling Analysis in Health Informatics and Bioinformatics 2*, 4 (2013), 213–223. 341

[40] HUMAIDI, N., AND BALAKRISHNAN, V. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR* (2012), vol. 35, IACSIT Press Singapore, pp. 1–6. 331, 333, 336, 347, 352

[41] HUMAIDI, N., BALAKRISHNAN, V., AND SHAHROM, M. Exploring user's compliance behavior towards health information system security policies based on extended health belief model. In *2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)* (2014), IEEE, pp. 30–35. 336, 340, 347, 352

[42] IBM. Ibm study shows data breach costs on the rise; financial impact felt for years, July 2019. Available from: `https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years`. 328

[43] ISO. Iso 27799:2016(en), health informatics information security management in health using iso/iec 27002, April 2017. Available from: `https://www.iso.org/standard/62777.html`. 335

[44] KEARNS, G. S., AND LEDERER, A. L. The impact of industry contextual factors on it focus and the use of it for competitive advantage. *Information & Management 41*, 7 (2004), 899–919. 336

[45] KHAN, R. A., AND KHAN, S. U. A preliminary structure of software security assurance model. In *Proceedings of the 13th International Conference on Global Software Engineering* (2018), pp. 137–140. 337

[46] KITCHENHAM, B., PRETORIUS, R., BUDGEN, D., BRERETON, O. P., TURNER, M., NIAZI, M., AND LINKMAN, S. Systematic literature reviews in software engineering–a tertiary study. *Information and software technology 52*, 8 (2010), 792–805. 337

[47] KOPPEL, R., SMITH, S., BLYTHE, J., AND KOTHARI, V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise*. IOS Press, 2015, pp. 215–220. 329, 330, 332, 333, 336, 347, 348, 351

[48] LEBEK, B., UFFEN, J., BREITNER, M. H., NEUMANN, M., AND HOHLER, B. Employees' information security awareness and behavior: A literature review. In *2013 46th Hawaii International Conference on System Sciences* (2013), IEEE, pp. 2978–2987. 347, 348, 351, 353

[49] LEWIS, B. How to tackle today's it security risks. *BSI Group* (2019). 330

[50] MARTIKAINEN, P., BARTLEY, M., AND LAHELMA, E. Psychosocial determinants of health in social epidemiology, 2002. 330, 333

[51] MCCORMAC, A., ZWAANS, T., PARSONS, K., CALIC, D., BUTAVICIUS, M., AND PATTINSON, M. Individual differences and information security awareness. *Computers in Human Behavior 69* (2017), 151–156. 347, 348, 353

[52] MCLEOD, A., AND DOLEZEL, D. Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems 108* (2018), 57–68. 337

[53] MOFFIT, R. E., AND STEFFEN, B. Health care data breaches: A changing landscape. *Maryland Health Care Commission* (2017), 1–19. 330, 332

[54] MORAIS, R. M. D., SOMERA, S. C., GOES, W. M., AND COSTA, A. L. Applicability of an assessment model for healthcare information systems in a public hospital. *JISTEM-Journal of Information Systems and Technology Management 13* (2016), 459–478. 337

[55] MORRISON, F., ZIMMERMAN, J., HALL, M., CHASE, H., KAUSHAL, R., AND ANCKER, J. S. Developing an online and in-person hit workforce training program using a team-based learning approach. In *AMIA Annual Symposium Proceedings* (2011), vol. 2011, American Medical Informatics Association, p. 63. 350

[56] NG, B.-Y., KANKANHALLI, A., AND XU, Y. C. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 4 (2009), 815–825. 336, 347, 348, 351, 353

[57] NOY, N. F., MCGUINNESS, D. L., ET AL. Ontology development 101: A guide to creating your first ontology, 2001. 336, 341, 352

[58] OKEKE, S. O., AND MABUZA, L. H. Perceptions of health care professionals on the safety and security at odi district hospital, gauteng, south africa. *African Journal of Primary Health Care & Family Medicine 9*, 1 (2017), 1–7. 336, 347, 352

[59] PARK, E. H., KIM, J., AND PARK, Y. S. The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security 65* (2017), 64–76. 336, 347, 352

[60] PARK, E. H., KIM, J., WILES, L. L., AND PARK, Y. S. Factors affecting intention to disclose patients' health information. *Computers & Security 87* (2019), 101340. 336, 347, 352

[61] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., AND ZWAANS, T. The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security 66* (2017), 40–51. 332, 333, 336, 347, 348, 353

[62] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. The development of the human aspects of information security questionnaire (hais-q). In *ACIS 2013: Information systems: transforming the future: Proceedings of the 24th Australasian Conference on Information Systems* (2013), RMIT University, pp. 1–11. 333, 347

[63] PETERSEN, K., VAKKALANKA, S., AND KUZNIARZ, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology 64* (2015), 1–18. 337

[64] PFLEEGER, S. L., PREDD, J. B., HUNKER, J., AND BULFORD, C. Insiders behaving badly: Addressing bad actors and their actions. *IEEE transactions on information forensics and security 5*, 1 (2009), 169–179. 329

[65] PREDD, J., PFLEEGER, S. L., HUNKER, J., AND BULFORD, C. Insiders behaving badly. *IEEE Security & Privacy 6*, 4 (2008), 66–70. 329

[66] PRISMA. Systematic reviews: Step 8: Write the review, 2018. xiv, 284, 337

[67] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 329, 330, 333, 334, 336, 340, 347, 351, 352

[68] SAMHAN, B. Security behaviors of healthcare providers using hit outside of work: A technology threat avoidance perspective. In *2017 8th International Conference on Information and Communication Systems (ICICS)* (2017), IEEE, pp. 342–347. 336, 340, 347, 352

[69] SEARCHHEALTHIT. Hospital takes aim at patient health data security with ai tools, July 2019. Available from: `https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/`. 328, 329

[70] SECURITYHIT. The 10 biggest healthcare data breaches of 2019, July 2019. Available from: `https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far`. 329, 351

[71] SEDLACK, D. Understanding cyber security perceptions related to information risk in a healthcare setting. 336, 347, 352

[72] SHAHRI, A. B., ISMAIL, Z., AND MOHANNA, S. The impact of the security competency on "self-efficacy in information security" for effective health information security in iran. *Journal of medical systems 40*, 11 (2016), 1–9. 336, 347, 352

[73] SHAHRI, A. B., ISMAIL, Z., AND RAHIM, N. Z. A. Constructing conceptual model for security culture in health information systems security effectiveness. In *Advances in Information Systems and Technologies*. Springer, 2013, pp. 213–220. 336, 340, 347, 352

[74] SHILTON, K., SUBRAMANIAM, M., VITAK, J., AND WINTER, S. Qualitative approaches to cybersecurity research. *IConference 2016 Proceedings* (2016). 329

[75] SHROPSHIRE, J., WARKENTIN, M., JOHNSTON, A., AND SCHMIDT, M. Personality and it security: An application of the five-factor model. *AMCIS 2006 Proceedings* (2006), 415. 332, 336

[76] SMITH, E., AND ELOFF, J. Cognitive fuzzy modeling for enhanced risk assessment in a health care institution. *IEEE Intelligent Systems and their Applications 15*, 2 (2000), 69–75. 330

[77] SONE, M., MIZUNUMA, K., NAKAJIMA, Y., YASUNAGA, H., AND OHTOMO, K. Job satisfaction, income, workload, workplace, and demographics of japanese radiologists in the 2008 survey. *Japanese journal of radiology 31*, 5 (2013), 364–370. 329

[78] TETZ, E. Network firewalls: Perimeter defense - dummies, July 2019. Available from: `https://www.dummies.com/programming/`

networking/cisco/network-firewalls-perimeter-defense/. 329, 331

[79] THEOHARIDOU, M., KOKOLAKIS, S., KARYDA, M., AND KIOUNTOUZIS, E. The insider threat to information systems and the effectiveness of iso17799. *Computers & Security 24*, 6 (2005), 472–484. 336, 340, 347, 352

[80] VAN DEURSEN, N., BUCHANAN, W. J., AND DUFF, A. Monitoring information security risks within health care. *computers & security 37* (2013), 31–45. 334, 336, 340, 347, 348, 350, 352, 353

[81] VERISON. Data breaches investigation report. 2019, July 2019. Available from: https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf. 329

[82] WHITMAN, M. E., FENDLER, P., CAYLOR, J., AND BAKER, D. Rebuilding the human firewall. In *Proceedings of the 2nd annual conference on Information security curriculum development* (2005), pp. 104–106. 1, 329, 331, 340

[83] WILLIAMS, P. A. In a 'trusting'environment, everyone is responsible for information security. *Information Security Technical Report 13*, 4 (2008), 207–215. 336, 347, 352

[84] WILLIAMS, P. A. When trust defies common security sense. *Health Informatics Journal 14*, 3 (2008), 211–221. 336, 347, 352

[85] WRIGHT, A., AARON, S., AND BATES, D. W. The big phish: cyberattacks against us healthcare systems, 2016. 330, 332

[86] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 330, 333, 335

[87] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 329, 331, 347, 349

[88] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 328, 330, 331, 332, 333, 335, 336, 340, 341, 352

Chapter 13

"Behaviour Coding Approach for Assessing Pitfalls in a Questionnaire Instrument towards assessing healthcare security Practice." (2022).

Prosper Kandabongee Yeng, Muhammad Ali Fauzi, Bian Yang

Abstract

This study, shares "pitfalls" to watch when preparing a questionnaire to assess the information security practice of healthcare staff that consists of multifaceted respondents. Hospitals are characterized by different respondents with varying domain knowledge such as knowledge in information security, information communication technology, and that of the domain knowledge in healthcare. It is therefore vital to prepare a questionnaire instrument for it to be well understood by all of the different categories of the healthcare workers else the quality of the study can be compromised. A synergy of conventional pretesting methods and behaviour coding were used to pretest the questionnaire.

Questionnaire problems including lack of understanding of healthcare information systems' structure, security and privacy concerns of respondents, the insignificant difference between questions, unclear items, complex questions, unrelated questions to respondents and incomplete response options were some of the identified pitfalls that could undermine the quality of the survey. Out of a total of 118 questionnaire items that were used in the pretesting, a total of 50 questionnaire items (representing 42%) were identified to have problems after the pretesting was conducted with a total of 36 respondents in behaviour coding and 21 respondents in conventional pretesting.

13.1 Introduction

Digitisation in healthcare transformed and improved on healthcare [49], however, it has also increased the attack surface [19] in the information security

(IS) domain. Technological countermeasures (such as firewalls, antivirus, intrusion detection, prevention systems, etc.) have traditionally been the default security solutions and have matured over time. These countermeasures are capable of safeguarding against unauthorised accesses to healthcare systems making it more difficult for the hackers to circumvent. As a result, the hackers have shifted their mode of nefarious operations. They gain unauthorized access into healthcare systems through the healthcare worker [68, 5] who is believed to be the easiest target and the weakest link in the security chain [68, 5].

In 2017, the healthcare system of the United Kingdom was heavily impacted by the Wannacry ransomware and this affected critical care [33, 24]. The ransomware spread to about 150 countries and affected about 230,000 computers in different sectors. Following that, in 2018, about 3 million healthcare records were compromised in Norway [73, 72] of which an insider aid was underscored. According to HealthCare IT News, there was another phishing attack that led to a breach of 38,000 patient records in Portland, Oregon-based Legacy Health in the United States in 2019. Personal data such as patients' email accounts, demographic information, dates of birth, health insurance data, billing details, medical data, Social Security numbers, and driver's licenses were stolen. Healthcare data breaches continue to increase sharply, with the passage of time. According to Verizon, globally, about 5 million healthcare records were compromised in 2017, followed by 15 million records in 2018 and 25 million records in the middle of 2019 which is threatening the quality of healthcare [66, 20].

Motivated by the security issues in healthcare, a comprehensive assessment of healthcare security is being carried out to determine if there are security practice gaps in healthcare. The study includes a survey that seeks to assess the psychological, social, and cultural factors of healthcare staff's in relation to their security practices [46, 71]. If there exists some non-conformance to security practice, various motivation schemes can further be explored to incentives for better security practice. To better understand the psychological, social and cultural effect on security practice, a comprehensive approach was adopted in the study. This consists of a mixed-method (qualitative and quantitative) survey consisting of a questionnaire instrument, interviews, and observing how healthcare staff comply with the security measures. To this end, a questionnaire was developed to measure for possible security gaps that might exist in the aspect of psychological, social and cultural context. The questionnaire was developed having adopted the stages in questionnaire design methods of rational, the prototypical, the facet design, the construct, the internal, and the external methods [47] [46]

One of the challenges is that the healthcare sector is characterized by various categories of study participants. For instance, in the information technology (IT) department in a healthcare setting, there could be IT offers

in which some are responsible for information security management, application development, IT project management, and network administration. Additionally, there are also healthcare professionals whose primary role is to offer healthcare services with the support of the IT systems. These healthcare staffs include doctors, nurses, pharmacies, laboratory personnel, and radiology personnel. Within the healthcare personnel, some of them may have professional knowledge in IT while others might have acquired basic IT skills, just enough to enable them to do their work. Furthermore, the healthcare sector consists of other supporting staff such as the health administrators, human resource personnel, finance, and accounting personnel, and they equally rely on the IT systems in the discharge of their duties. Since human factors can influence the security practice of all these categories of staff, the survey study aimed to include them in the research. The problem is how can the questionnaire instrument be scaled such that it can be well understood by all these variant participants? Furthermore, the study area includes Ghana, Norway and Indonesia where the healthcare delivery culture and the level of IT setup could vary. Therefore, how can a questionnaire be developed to be understandable for all the participants in these countries? To answer these questions, the goal of this study is to identify and use various questionnaire design and pretesting methods in developing a clear questionnaire to ensure that the questionnaire items in the survey are well understood by the multifaceted respondents. This will enable them to provide good responses for an effective and reliable study. To this end, the specific objectives are captured in the research specific aims and objectives section.

13.1.1 Research aim, objectives and hypotheses

Due to IT knowledge gaps across these categories of healthcare staff, developing a questionnaire to effectively measure the security practice while reducing response burden, require a multifaceted design and pretesting strategies to balance the understanding of the constructs and all questionnaire items among the respondents. For instance, a nurse who studied IT security at the bachelor or master level will have a higher level of understanding of some terminologies in an information security questionnaire items than a colleague nurse who has been trained on how to only use the IT systems to do their work. Besides, the questionnaire items need to be structured to have a common denominator that can be able to efficiently examine the security practice across the multifaceted categories of respondents in their respective healthcare roles. Moreover, various hospitals in different countries may have different IT setups in their hospitals. In scenarios wherein one country, the hospitals only operate on local area network while in some other countries, the hospitals operate on a wide area network with the support of the internet, the questionnaire items then need to be scaled to have a common

denominator for the assessment of the security practice of healthcare staff across such variances. Based on this background, the hypothesis is that:

- H1: The questionnaire instrument that was developed to measure the security practice of healthcare staff on the aspect of psychological, social and cultural effect is paradigmatic.

It is assumed in this null hypothesis that each of the questionnaire items is well understood, has no complex terms, errors or issues of social undesirability that may lead to wrong responses or refusal by the participant to respond to any of the questionnaire items.

To answer this hypothesis, a pretesting of the questionnaire need to be conducted. There are various pretesting methods for questionnaire instruments. The research question here is:

- Q1: Which of the questionnaire design methods should be adapted to effectively design questionnaires for analysing security practice in healthcare?

- Q2: Which of the questionnaire pretesting methods should be adapted to effectively and comprehensively assess the questionnaire instrument?

The objective of this study was to first surveys for the various questionnaire design pretesting methods for developing and pretesting the questionnaire. The selected method(s) were then assessed for their suitability for designing and pretesting the questionnaires. Spontaneously, the answer of the hypothesis (H1) would be determined from the pretesting analysis.

Section 2 showed how the design and pretesting methods were selected, assessed and used for the designing and pretesting. Section 3 presents various questionnaire design methods and how they were used in the development of our security practice questionnaire. Section 4 and section 5 respectively presented the pretesting findings and discussions.

13.2 Our Approach

The aim of this paper was to effectively design and pretest a questionnaire to improve the response quality of a questionnaire that is intended to be used for analysing healthcare security practices. Literature concerning questionnaire design and pretesting methods were therefore surveyed in Google scholar, IEEE Explore, PUBMED, Science Direct, Elsevier, and SCOPUS. The keywords which were used in the survey include Questionnaire design, Questionnaire pretesting, Information security, and healthcare with boolean functions of AND, OR, and NOT.

Each of the questionnaire design and pretesting methods was assessed and considered for the design and pretesting of the healthcare security practice. The assessment of the design methods was related to the objective and scope of the healthcare staff security practice analysis, modelling and incentivisation (HSPAMI) [73, 71] in relation to the psychological, social, and cultural context. Guided with the questionnaire design methods the questionnaire was first developed and subsequently pretested with selected pretesting methods having assessed their objective, pros and cons.

13.3 Questionnaire design Methods

A questionnaire is the most widely used instrument for gathering data on knowledge, attitude, opinion, behaviour, facts, etc., concerning people, objects, and events [53, 38]. The questionnaire tool is usually developed to collect information from the respondents. Various questionnaire design methods such as the rational, the prototypical, the facet design, the construct, the internal, and the external methods are usually adopted [47, 67, 46, 35, 34, 6] as shown in 13.1.Additionally, there are four stages involved in questionnaire development: These are concept analysis, item reproduction, scale construction, and evaluation. Each of the questionnaire design methods and how they are applied to these stages is shown in table 13.2.

The rational method [47] relies solely on the knowledge of the questionnaire developers or expert's judgment to place the questionnaire items [2, 67]. So the experts mostly consider in their perspective, what is rational or reasonable based on their knowledge in the problem domain. The experts' knowledge in placing the questionnaire item is usually guided by the face validity, to determine if a questionnaire looks valid to measure the desired construct of interest from the opinion of the expert or developer, respondents, and other observers who are technically untrained.

The prototypical method is based on a theory from cognitive science called prototype theory. It is about the presentation of categories such that the variation of members of a category degrades away from the centre [47, 67, 6, 23]. So the objects or members of a class are mostly related to that class. Literally, the prototypical approach is like clustering of the questionnaire items where the items members of a category vary in characteristics. So members that are more related (more prototypical) to a category or a class are easier to be categorized. In the test construction stage of a questionnaire, each construct is represented by a set of acts or behaviour that are more prototypically related or central to that construct. The prototypical approach concentrates on placing items under the constructs that are more related in characteristics and this increases the cognitive processing of respondents thereby, increasing the quality of the questionnaire instrument. The construction is usually guided by the informal knowledge and experience of

the respondents [10, 55]. In the item production stage of the questionnaire, members of the target population are given the option to nominate experts with vast knowledge in the construct, to outline behaviours that relate to this construct. To preserver, the expert's input, the editing of the expects' constructs by the questionnaire developers is highly limited.

The construct method [47, 46, 35, 34] is primarily derived from a theoretical approach in which the constructs are developed from the theoretical concept of the research domain. Hypotheses about the questionnaire are then developed and assessed empirically. if the questionnaire items or scales are found to deviate from the construct theory, new construction of the items and scales are formed by revising the questionnaire. The concept analysis of the construct method relies on the guidance of the construct theory, in which a nomological network with relevant variables (independent, mediating, and dependent) and their respective relationships among the variables are often used. The related variables usually have correlation with the construct in the study [47, 46, 35, 34].

The facet design method [47, 46] uses the principle of content validity. It adopts a comprehensive and systematic approach to analyze and specify the constructs toward ensuring that the items in the questionnaire significantly represent the construct. The process begins with a comprehensive catalog of the construct domain which are then categorized into various sections referred to as the facet [32, 31]. Each facet is further expanded into facet elements. The facet design method is also a hypothesis testing method with empirical tests much like the construct method. But this method differs from the construct method in the sense that it does not primarily depend on a formal theory of the construct. It only requires formal knowledge of the construct and goes through four steps in the concept analysis phase. These include taking an inventory of the behavioural features and their underlying processes that are relevant to the construct. An example is a security practice that has psychological, social, cultural, and demographic factors. To ensure content validity, all these aspects need to be represented in a questionnaire in a typical study on security practice as shown in the independent variables of Figure 13.1.

Secondly, the facets are designed to be mutually exclusive by expanding the inventory. For instance, the psychological facet of the construct may be expanded to include psychological attributes such as perceived severity, perceived vulnerability, and perceived efficacy. In the third step, the questionnaire items of each facet can then be determined to cover the content domain. Finally, the various items in each facet are then combined to form the formal structure [61].

In the internal method [47, 46, 9, 11, 64], constructs cannot be specified in advance. Constructs are formed or derived from empirical relations between questionnaire items. The co-variance among a set of questionnaire

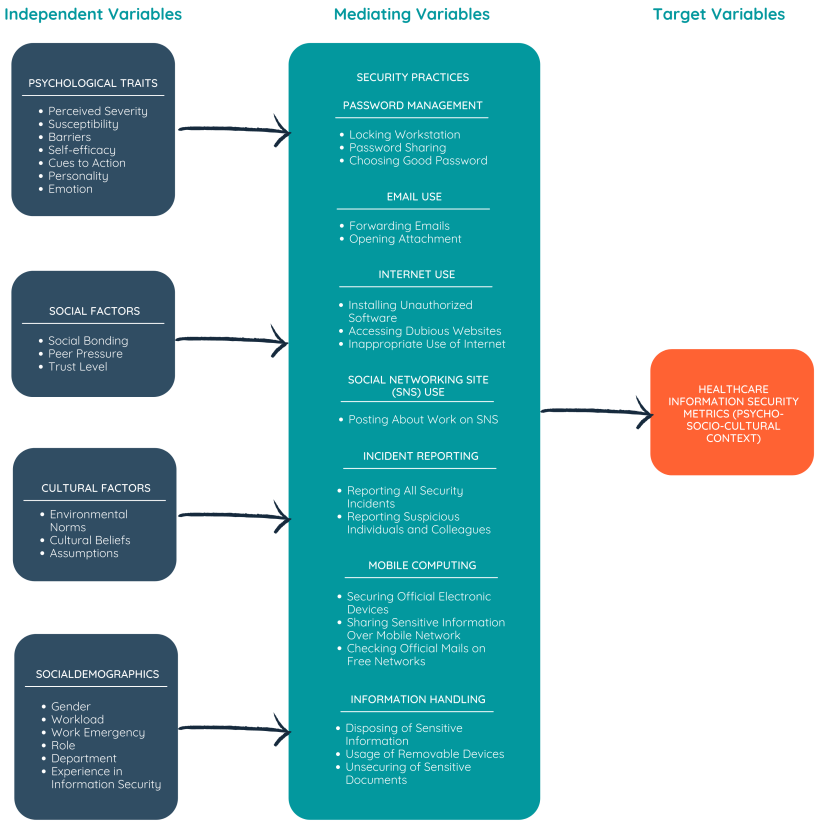


Figure 13.1: Nomological network with independent, mediating and dependent variables.

items is due to a common factor and that is considered as the underlying construct. The internal method is largely used to improve upon the existing questionnaire instrument. It can also be used to create a new questionnaire from a pull of questionnaire items in the same domain. Since the construct is not pre-specified in the internal method, the concept analysis stage of a questionnaire is often skipped. So the question construction often begins with the item's production.

The external method[47, 46, 42] fundamentally relies on the principle that individual responses to a questionnaire item represent their respective

behaviour that may be related to many non-test behaviours. The statistical relationship between the items responded to and the specified behaviour is therefore considered to be more informative. The construction does not require theories or concept specification but the concepts are obtained through the predicted or determined non-test behaviour or criterion and not through psychological theories. A collection of heterogeneous items that are related to the criterion are gathered at the item production stage. The item pool consists of heterogeneous items of which the diverse items are very important. The many different aspects of the items in the items pools significantly contribute to the production of non-test behaviour. The strength of the relationship between items and the study area (criterion) is much focused on the scale construction stage.

A summary of the methods and their objectives are shown in Table 13.1. The questionnaire design methods are usually applied at various stages of the design as shown in Table 13.2. The concept analysis is the initial stage of the questionnaire construction. So the theoretical framework is identified together by outlining and defining the constructs. Primarily, the concept stage

Table 13.1: Questionnaire Design Methods and Objectives.

Method	Objective
Rational	Most applicable when little formal knowledge of the concept is known or when the concept has not been explored in details
Prototypical	It is aimed towards increasing the cognitive process of respondents. Therefore, more prototypical items would be better understood
Facet	The intention of this method is to ensure that the questionnaire items comprehensively represent the constructs. This is achieved by systematically outlining the constructs with the guidance of content validity
Construct	The construct method aimed towards designing questionnaire items to meet the construct theory. This is done by relying on formal knowledge to generate a hypothesis of the items for empirical assessment
Internal	The method is intended for improving upon existing questionnaires or developing new questionnaire items from existing questionnaires that are related. This is done by observing the common factor or co-variance among the items
External	This method aimed towards a generalization of the questionnaire with an external criterion by gathering and analyzing for the strong relation of heterogeneous items that are related to the construct and the external criterion

includes the specification of the purpose, objectives, research questions, and hypotheses [53]. At this stage, the respondents' background needs to be understood and a clear understanding of the problem needs to also be explored through literature reviews.

Table 13.2: Questionnaire design methods and their applications in the various design stages

Design Methods	Questionnaire design Stages			
	Concept Analysis	Item Production	Scale Construction	Validation
Rational	The theoretical framework of the concept is usually originated from the ideas of the questionnaire developer; Concepts are obtained in a typologies syndrome or global descriptions.	Uses intuitive or informal criteria in the item production; Items are produced using typologies, syndrome and global description.	Scale construction is based on the developer's judgement	Items are assessed based on face validity. Estimates of the validity and reliability are also evaluated.
Prototypical	-	Item production is based on act-nomination. Thus persons with extreme knowledge of the construct are selected to outline behaviours that illustrate the construct. Developers of the questionnaire are not required to make significant changes.	Prototypical ratings are used to select the questionnaire items	Peer rating procedure is used in the evaluation [14, 1].
Facet	The following steps are followed: An inventory of the behavioural factors and underlying processes of the constructs are taken; The facet is defined through the elaboration of the inventory; The facet elements are then determined to be mutually exclusive; The item in each facet are then combined to form the final study.	The total number of items needed depends on the size of the facet design per facet. Content is then created for each facet element.	Items with high correlation to the intended scale are optimised for used	Network confirmatory factor analysis, reliability analysis and different item function
Construct	This is guided by the construct theory, expressed in a nomological network, using relevant variables to indicate their relationship, as shown in Fig 1.,	The operational definition of the construct in the study is used to generate the items. Experts and potential respondents can judge the items	Scale construction is based on the content saturation ie the convergence and discriminant validity of the items. Items with high correlation to the intended scale are optimized for use	-
Internal	-	Items are selected to be relevant to the content domain with a degree of content homogeneity. The existing set of items is often selected similar content domain.	The focus is on the homogeneity of items. Homogeneous items are then interpreted post-hoc with their respective scaling. Non-homogeneous items are excluded	Stability of identified item co-variance structure is mostly assessed using cross-validation and confirmatory test
External	-	Collection of heterogeneous items that are relevant to the criterion is obtained[22]	The strength of the relationship between and criterion are used. Items with higher correlation with the criterion but low correlation among them are optimal	Cross-validation is used for item-criterion and scale-criterion assessment. Test-retest is also used.

The item production stage, which is also referred to as the questionnaire conceptualization stage [53], involves gathering the questions or obtaining a pool of the questionnaire items based on the initial specification in the con-

cept analysis stage. In this phase, the items can also be reviewed by experts or potential respondents. The content of the questionnaire (eg. the questions) is developed by specifying whether the questionnaire is intended to measure either knowledge, attitudes, perceptions, opinions, recalling facts, behaviour change, etc. Variables including independent, mediating, and dependent variables are also specified. Essentially, pretesting of the questionnaire can be conducted at this stage and the findings can be used to subsequently update or revise the questionnaire items. Meanwhile, in the scale construction stage, possible answers to each questionnaire item are selected for the scales while relying on options that increase the psychometrics (mental capacity and processing) of the study. Having a good understanding of the collected data and the suitability of the data analysis method is very necessary. Therefore a preliminary statistical analysis method should be tested to ensure that the results will meet the needs of the study objective.

The final step involves the evaluation of the questionnaire which consists of establishing validity and reliability. Validity here refers to the measure of what the questionnaire claims to be measuring [53, 38]. Validity can be reduced if a higher proportion of errors are systematically built on the questionnaire instruments. The types of validity include content, construct, criterion, face, internal, and external validity.

Internal validity is concerned with the effectiveness of the results within the scope of the study. It has to do with causality, i.e. the assignment of causes to outcomes. External validity is the extent to which the study can be applied or generalized beyond the current study scope. A construct is a concept being measured by a test. So construct validity is a test to assess if the study is measuring the construct it was designed to measure[36, 37]. A higher number of different measures increases the construct validity on the condition that the measurements are all measuring the same concept or construct in the study. Construct validity is mostly assessed by comparing the study to other tests that measure similar qualities to determine the correlation between the two studies. Content validity is when a study measures the knowledge of the content domain of which it was designed to measure. For instance, if a study was designed to measure information security practice in healthcare, the content validity assesses if the study was indeed measuring information security practice and not measuring something else outside security practice such as computer use. Furthermore, if the study area is about information security practice, the content validity criteria are met when the questionnaire items have comprehensively covered all the knowledge areas of information security practice [36]. Face validity involves the assessment of the questionnaire to determine if the test appears valid to the respondents, the administrator of the questionnaire [36]. Criteria validity is a measure that seeks to determine how well a test can predict the outcome of another measure[36]. An instance includes how well can the results of the informa-

tion security questionnaire be used to sufficiently provide incentivization methods to improve upon the security-conscious care behaviour of users. Another example is how well a security practice questionnaire results will be used to correct the challenges often faced by healthcare staff as they go about with their usual duty [36, 37]. A panel of experts and field tests can be used to assess the validity.

13.4 Pretesting methods

Pretesting aims to identify ambiguous questions or wording, unclear instructions, and other issues with the questionnaire prior to actual use [51, 13]. It helps to also provide information concerning reliability and validity by identifying potential problems before the actual use of the instrument. So the pretesting of the survey instrument should be fully described. The types of pretesting include conventional pretesting, cognitive interviews, behaviour coding, response latency, vignette analysis and, formal response debriefing. Other types of pretesting include focus groups discussion, experiment and statistical modelling [51, 8, 43, 12, 58, 18, 13] as summarized in Table 13.16.

13.4.1 Conventional pretesting

Conventional pretesting of the questionnaire is based on the assumption that the problems of the questionnaire are identified based on issues raised by respondents. Respondents may refuse to answer such items or indicate their lack of knowledge of the item. In conventional pretesting, there are no exact tests but the testing is based on subjective views of respondents which are translated or transcribed by the fieldworkers or interviewers[51, 8, 43] and this can make it difficult to understand the full problems raised by the respondents. Moreover, in the debriefings of the interviews in conventional pretesting, there is no scale to illustrate the severity of the described problems. Therefore, researchers only rely on intuition and experience to judge the seriousness of the problems and decide on what to address [51]. Additionally, respondents may be hesitant, uncomfortable, or showed visible resistance in answering the questions which interviewers can note down during the debriefing session [51] but this will require the presence of the researcher during the response process. This requirement, therefore, drifts into a cognitive interview.

13.4.2 Cognitive interviews

The cognitive interview involves drawing out the view or depicting the processes in answering questions. This is towards analyzing to extract the exact problems associated with the questions [51, 8, 43, 12, 41, 58, 18, 13, 52]. The

intention is to reveal the thought processes in interpreting and answering a question.

The methods employed in cognitive interviewing include verbal probing (concurrent and retrospective), observing the respondent's behaviour and think-aloud, or read-aloud while the respondent answers the questions in the questionnaire instrument [58, 18].

The probing involves asking the respondents to interpret the questions and to provide an understanding of the meanings of words used in the questions. The respondents also explain their responses and pinpoint areas of the questionnaire that has difficulties in understanding, interpreting, or completing [39, 13, 69]. The fundamental goal is to clarify the understanding of respondents' on the questions.

Observational aspect in cognitive interviews includes observing respondents skipping questions, flipping a page back and forth, placing answers in the wrong fields of the questionnaire form. The observation also includes changes in appearance such as frowning and hesitation. In this regard, the respondent can be directly questioned about the difficulties they are facing with each question on the questionnaire.

In the think-aloud method, the researcher aims to understand the cognitive processes used by the respondents in answering the questions. So the researcher encourages the respondents to speak out their thoughts while answering the questionnaire instrument [13, 59, 63].

In a related study, Cantril and Fred used one or two written probes to assess the understanding of survey questions from respondents. Similarly, Balson used none directional probing to explore seven questions that were previously responded to through ordinary interviews. Ordinary interviews aim to obtain just the responses to the questions [51]. Retrospective probing was used by the interviewers to extract the cognitive process employed by respondents to arrive at their answers in their previously responded questioned which ordinary interview was used. Belson's hypothesis was that respondents could reconstruct their thought process from their previously answered interview. Belson's study [15] did not have much impact on pretesting practice due to the adoption of labor-intensive in the study. Subsequently, the cognitive interview became popular after think-aloud was used to answer survey questions about past events [51, 56]. Cognitive laboratories were also created towards understanding responses to the survey questionnaire [51].

Results of cognitive methods that involve verbal reporting of information in short-term memory are likely to be real if the verbalization does not involve further explanation that has the potential to alter the thought process [51, 27]. But the general use of verbal report methods in cognitive processes for answering survey questionnaires is difficult to justify particularly for tests that fail to meet the conditions for valid verbal reports such as term

comprehension. Although the social interaction between respondents and interviewer in a cognitive interview may violate key assumptions [51, 27], a certain kind of verbal probing poses difficulties for respondents. Respondents do not have any difficulties with re-orienting probes (asking for an answer). However, respondents have difficulties elaborating probes (asking for further information). Also, a cognitive interview is much directed by the interviewer and as a result, the outcome can be biased from the interviewer interference and this could fail to support the inquiry.

13.4.3 Experimental methods

Supplementary methods to conventional pretesting and cognitive interviews can both identify various problems of a questionnaire instrument. This leads to a revision and redesign of the questionnaire to address the identified problems. But how will it be known if the revisions are an improvement to the old questionnaire? An experimental comparison of the original and the updated version is used. One way of the experimental comparison is to compare the original and the updated versions of the questionnaire, using the initial test methods which were used in the pretesting of the original version [51] to identify the problem. For instance, if conventional pretesting was supplemented with response latency to identify problems with an item, that item and its revised version can be tested again with the conventional pretesting and any supplemented method (such as response latency) which was used. This is to ascertain if the revised version indeed had fewer problems. Furthermore, the original and the updated version of the questionnaire can be tested to determine if there is a difference in the survey estimates.

13.4.4 Behaviour coding

Behaviour coding involves observing subsets of the respondents' and interviewer's verbal behaviour by monitoring interviews or reviewing recorded interviews of their question asking and answering interactions [51, 45]. Questions found to be scoring high frequency (15% or above of the respondents) in a certain behaviour (such as the respondent needed clarification or the interviewer failed to read the question verbatim) are noted to need repairs. Aside from the frequency count in certain behaviour, the sequence of a question's behaviour coding is coded as either paradigmatic, problematic, or inadequate [51, 65] as detailed in Table 13.3.

Paradigmatic involves a question coding where the interviewer correctly reads the question, the respondents select one of the offered alternatives, then the interviewer codes the answer as being correct and this is also referred to as adequate answering as shown in Table 13.3. Problematic codes mean that the sequence was non-paradigmatic but the issue was resolved.

For instance, the respondent asked for clarification, and then selected one of the offered alternatives. Inadequate coding is also non-paradigmatic but the identified problem remains unresolved. Questions with a high proportion of non-paradigmatic sequences such as inadequate answer, don't know, or refused to answer are also tagged as needing repairs.

13.4.5 Response latency

Response latency is another testing method that has to do with the number of times a respondent takes to answer a question [17]. Longer delays in response latency signify uncertainty in the response of the respondent's answer and this inadvertently evaluates questions by themselves. Certainly, the interpretation of the response latency is not straightforward because a long time needed may be due to careful processing instead of difficulties in interpreting the questions.

13.4.6 Respondent debriefing

Respondent debriefing involves the incorporation of follow-up questions in a standard interview [51, 52]. The respondent is duly informed about the purpose of their response inquiry [51]. In pretesting questionnaire with

Table 13.3: Behaviour codes [13]

Behavior Type	Meaning
Reader/Interviewer behavior Codes	
Exact (E)	Interviewer exactly read the questionnaire item
Slightly Changed (S)	Interviewer made minor wording changes when reading the question
Major Changed (M)	Interviewer made significant wording change when reading the question
Respondent behavior	
(1) Interruption with answer	Respondent interrupted the question reading to give his or her answer
(2) Clarification	Respondent asked for clarification
(3) Adequate Answer	Respondent provided answer after question reading
(4) Qualified answer	Respondent qualified his or her answer
(5) Inadequate answer	Respondents initial answer was inadequate
(6) Don't Know	Respondent gave a "don't know" response
(7) Refusal to answer	Respondent refused to answer the question

respondent debriefing provides knowledge on the meaning of the questions and the reactions of the respondent to the question [51].

13.4.7 Vignettes

Vignettes[51] involve hypothetical scenarios that respondents assess and this may be conducted in either undeclared or participating pretesting methods. Vignettes approach is more suitable for exploring how people think about concepts; testing the consistency of the interpretations of the respondents, testing the consistency of the interpretations of the concepts of a respondent, assessing the dimensions associated with a concept, and assessing other questions word problems.

13.4.8 Focus group

When the construct and objective of a questionnaire are set, a focus group is then formed to meet. The group then assesses respondents. Areas of the questionnaire with issues are required to be listed. The understanding of tasks such as keywords, concepts, recalls of respondents, question-wording, etc are assessed by the group [40].

13.4.9 Expert reviews

Expert review is among the commonest methods in questionnaire pretesting and it involves individual or group sessions of experts who completely rely on the expertise to identify problems in questionnaire items[69, 70, 28]. The experts usually follow a structured appraisal system or rely on their own judgment to identify the questionnaire problems.

13.4.10 Statistical modelling

Statistical models such as latent class analysis(LCA) [51, 50] and item response theory (IRT) [51, 54] can be used to estimate the errors in questionnaire instrument. LCA is similar to clustering that identifies hidden subgroups in a population in which the subgroups are unique to each other but have similar members or objects. When the questions have been answered by the same respondents two or more times, LCA can be used to analyze and estimate the errors associated with the questions as described in [50]. IRT determines a way of testing the understanding of respondents by collecting answers from each respondent and indicating whether their respective answers were correct or not. The results are then organized to indicate each respondent and the status of their respective responses (correct answer or wrong answer). The data is then analyzed towards improving upon the questionnaire [21].

13.5 Pretesting results

Having assessed and identified the questionnaire design and pretesting methods as shown in Table 13.16 and Table reftable: Pretestingtechniques respectfully, a number of them were suitable for designing and pretesting a questionnaire towards analyzing healthcare security practice. This questionnaire was then pretested with conventional pretesting, and behaviour coding. The findings of conventional pretesting are shown in Table 13.4.

A total of 21 respondents answered the questionnaire in the conventional pretesting approach and provided feedback on various issues which were categorized to include an arrangement of questions scales (19%), incomplete response options (19%) and unclear questions (19%) as shown in Table 13.4. A relatively high number of respondents (23.8%) opined on complicated terms in the questionnaire items.

Table 13.4: Conventional pretesting findings

#	Questionnaire issues identified	Count of Respondents	%
1	Arrangement of questions scales	4	19.0
2	Incomplete response options for respondents	4	19.0
3	Understanding of information systems' structure of hospitals	2	9.5
4	Use of abbreviations which are not understood by all respondents	3	14.3
5	Questions that are unrelated to the responsibilities or task of respondents	1	4.8
6	Unclear question	4	19.0
7	Complicated terms for respondents eg multi-factor authentication	5	23.8
8	Insignificant difference between some questions	4	19.0
9	Security and privacy need of respondents in relation to the questionnaire tool	1	4.8
10	Grammatical errors and spelling mistakes	3	14.3

13.5.1 Behaviour coding results

A total of 36 respondents were interviewed in the behaviour coding method. The questionnaire instrument has a total of 118 questionnaire items in 6 different sections. The questionnaire was first revised in English based on the results from the conventional pre-testing. Since the same questionnaire was

to be answered in Norwegian and in the Indonesian language, it was translated into these languages. The pretesting was done in Ghana, Norway, and Indonesia by respondents who had healthcare backgrounds and were not working with the hospitals in which the actual study was to be conducted. Among the 36 respondents, 10 of them were interviewed in English, 7 of them preferred Norwegian and 19 of them were interviewed in the Indonesian language. So a total of 4,248 (36 respondents * 118 questionnaire items) coded behaviour were collected from the respondents and the interviewers. The results are based on the responses across the three languages (English, Norwegian, and Indonesian).

13.5.1.1 Respondent behaviour types

The table 13.5showed the codes of the respondent's behaviour types and the quantification of the responses from the respondents. Out of the 4,248, 3,923 responded with adequate answers (3). This represents about 92.35% of the total responses. A total of 262 responded with clarification (2) and this represented 6.17% of the total responses. None of the respondents refused to answer any of the questionnaire items as shown in Table 13.5.

Table 13.5: Proportion of respondent behaviour types

Behaviour Types Codes	Respondent behavior counts	%
1 Interruption with answer	5	0.12
2 Clarification	262	6.17
3 Adequate answer	3923	92.35
4 Qualified answer	51	1.20
5 Inadequate answer	1	0.02
6 Don't know	6	0.14
7 Refusal to answer	0	0.00

Various questionnaire item numbers and the number of respondents who answered with interruption (1) in all the three languages are shown in Table 13.6. The total number of persons who responded with an interruption for each item was not up to 15% or more. Question 1.B2 in section B, part 3 has a maximum of 2 respondents who answered with interruption.

Out of the 262 responses who sorted for clarifications, a total of 14 questionnaire items were answered by 15% or more respondents with clarification as shown in Table 13.7. Question number 1.A in part 4, Section A has the highest proportion of respondents (33%) who answered with clarification. Furthermore, questionnaire item number 1.B2 in part 4, Sect A, num-

Table 13.6: Proportion of respondents who answered with interruption (1) in all languages (English, Norwegian and Indonesia

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 3	Section B	1.B2	2	6
2	Part 3	Section D	1a.B2	1	3
3	Part 5	Section A	1.A	1	3
3	Part 5	Section A	1.B2	1	3

ber 5.k in part 4, Sect B, and questionnaire item number 14 in part 4 section B each as the next highest proportion (22%)of respondents who answered with clarification.

Table 13.7: Proportion of respondents who answered with Clarification (2) in all languages (English, Norwegian and Indonesia

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 1	Section A	4	6	17
2	Part 3	Section A	1.K	6	17
3	Part 4	Section A	1.K	6	17
4	Part 4	Section A	1.A	12	33
5	Part 4	Section A	1.B	7	19
6	Part 4	Section A	1.B2	8	22
7	Part 4	Section A	3.A	7	19
8	Part 4	Section B	4.K	6	17
9	Part 4	Section B	4.B	7	19
10	Part 4	Section B	5.K	8	22
11	Part 4	Section B	5.A	6	17
12	Part 4	Section B	5.B	7	19
13	Part 4	Section B	5.B2	6	17
14	Part 4	Section B	14	8	22

The table 13.8consists of proportions of the respondents who did not answer exactly the respective questions in the administered questionnaires. Out of a total of 36 respondents who answered the questionnaires in English, Norwegian and Indonesian language, 15% or more of the respondents did not provide exact responses. A total of 22 questionnaire items were not adequately responded, out of a total of 118 questionnaire items. Questionnaire item 1.A in section A part 4 have the highest proposition (57%) of respondents who did not exactly respond to the item.

Table 13.8: Proportion of respondents (out of 36 respondents) who did not answer exact in all languages (English, Norwegian and Indonesia)

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 1	Sect A	4	6	17
2	Part 3	Sect A	1.K	6	17
3	Part 3	Sect E	1	6	17
4	Part 4	Sect A	1.K	6	17
5	Part 4	Sect A	1.A	13	36
6	Part 4	Sect A	1.B	7	19
7	Part 4	Sect A	1.B2	9	25
8	Part 4	Sect A	3.A	7	19
9	Part 4	Sect B	4.K	10	28
10	Part 4	Sect B	4.B	7	19
11	Part 4	Sect B	5.K	9	25
12	Part 4	Sect B	5.A	7	19
13	Part 4	Sect B	5.B	7	19
14	Part 4	Sect B	5.B2	7	19
15	Part 5	Sect A	3a	7	19
16	Part 5	Sect B	14	8	22
17	Part 6	Sect A	10	7	19

Regarding response with qualification, out of the total number of 51 response behaviours which were counted as shown in Table 13.5 and Table 13.9 none of the questionnaire items got 15% or more of the 36 total number of respondents who answered with qualification. The high number of proportions of respondents who answered with qualification was about 11.1% and they responded to question 4.K in Part 4 and Section B and question 3a in Part 5 and section A.

Table 13.10also presents the proportion of respondents who answered with the "Don't know" code (6). From the responses, none of the questionnaire items also have 15% responses out of the total responses.

13.5.1.2 Presentation of results based on the languages

As the questionnaire was administered in 3 languages, a gist of the results is therefore presented in this section in those 3 languages thus English, the Indonesian language and Norwegian language. Overall, 19 persons responded to the questionnaire in the Indonesian language, 10 persons responded in English, and 7 persons answered in Norwegian, bringing the total number of respondents to be 36.

Table 13.9: Proportion of respondents who answered with Qualification (4) in all languages (English, Norwegian and Indonesia)

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 1	Sect A	1	3	8.3
2	Part 1	Sect A	2	1	2.8
3	Part 1	Sect A	7	2	5.6
4	Part 3	Sect B	1.B	3	8.3
5	Part 3	Sect C	1.K	3	8.3
6	Part 3	Sect D	1	1	2.8
7	Part 3	Sect E	1	2	5.6
8	Part 4	Sect A	1.A	1	2.8
9	Part 4	Sect B	1.K	1	2.8
10	Part 4	Sect B	2.B	3	8.3
11	Part 4	Sect B	3.A	1	2.8
12	Part 4	Sect B	4.K	4	11.1
13	Part 4	Sect B	5.K	1	2.8
14	Part 4	Sect B	5.A	1	2.8
15	Part 5	Sect A	1.A	1	2.8
16	Part 5	Sect A	3a	4	11.1
17	Part 5	Sect B	3	2	5.6
18	Part 5	Sect B	4	3	8.3
19	Part 5	Sect B	6	2	5.6
20	Part 5	Sect B	8	2	5.6
21	Part 5	Sect B	9	1	2.8
22	Part 5	Sect B	10	2	5.6
23	Part 5	Sect B	12	1	2.8
24	Part 5	Sect B	16	1	2.8
25	Part 5	Sect B	17	2	5.6
26	Part 6	Sect A	9	1	2.8
27	Part 6	Sect A	10	2	5.6

With regards to responses in the Indonesian language, the 118 questionnaire items were exactly read to all the respondents. However, not all the responses were exact. Questionnaire items that were not answered exactly by more than 14% of the respondents are shown in Table 13.11. From this table, 10 questionnaire items were not exactly respondents by 32% or more of the respondents. Questionnaire number 1.A in part 4, section A, 1.B in part 4 and section A and 5.k in Part 4 and Section B showed the highest proportion of respondents who did not answer exactly.

With regards to English responses, Table 13.12 showed 31 questionnaire

Table 13.10: Proportion of respondents who answered with Don't Know (6) in all languages (English, Norwegian and Indonesia)

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 4	Section A	1.B2	1	3
2	Part 4	Sect B	1.K	1	3
3	Part 4	Section B	5.B2	1	3
4	Part 5	Sect B	3	1	3
5	Part 5	Sect B	4	1	3
6	Part 5	Sect B	11	1	3

Table 13.11: Proportion of respondents In Indonesia (out of 19 respondents) who did not answer exact

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 1	Section A	4	6	32
2	Part 4	Section A	1.K	6	32
3	Part 4	Section A	1.B2	6	32
4	Part 4	Section A	1.A	7	37
5	Part 4	Section A	1.B	7	37
6	Part 4	Section B	4.K	6	32
7	Part 4	Section B	5.K	7	37
8	Part 4	Section B	5.A	6	32
9	Part 4	Section B	5.B	6	32
10	Part 4	Section B	5.B2	6	32

items in which 15% or more of the respondents did not respond with exact (3).

With regards to the questionnaire item in Norwegian, 7 persons responded to the questionnaire, and out of the 118 questionnaire items, all of them were exactly read to the respondents. However, 11 questionnaire items were not exactly respondents by 2 or more respondents as shown in Table 13.13. This means that over 14% of the respondents of the Norwegian version of the questionnaire did not give straight-away answers to 11 of the questionnaire items.

13.5.1.3 Summary of reading

With regards to the reading of the questionnaire which was responded in all the three languages (English, Norwegian, and Indonesian), out of 36 times that the questionnaire was read to the 36 respondents, 5 questionnaire items

Table 13.12: Proportion of respondents In English (out of 10 respondents) who did not answer exact

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 1	Section A	1	3	30
2	Part 1	Section B	8	2	20
3	Part 2	Section A	9	2	20
4	Part 2	Section A	10	3	30
5	Part 3	Section A	1.K	3	30
6	Part 3	Section B	1.K	2	20
7	Part 3	Section B	1.B	2	20
8	Part 3	Section B	1.B2	4	40
9	Part 3	Section C	1.K	3	30
10	Part 3	Section C	2.B	3	30
11	Part 3	Section D	1	2	20
12	Part 3	Section E	1	4	40
13	Part 4	Section A	1.A	4	40
14	Part 4	Section A	1.B2	2	20
15	Part 4	Section A	2.K	3	30
16	Part 4	Section A	2.A	4	40
17	Part 4	Section A	1.B2	2	20
18	Part 4	Section A	3.B	2	20
19	Part 4	Section B	1.K	2	20
20	Part 4	Section B	4.K	2	20
21	Part 4	Section B	4.A	2	20
22	Part 5	Section A	3a	3	30
23	Part 5	Section B	3	2	20
24	Part 5	Section B	4	3	30
25	Part 5	Section B	6	3	30
26	Part 5	Section B	11	2	20
27	Part 5	Section B	14	3	30
28	Part 6	Section A	3	3	30
29	Part 6	Section A	6	2	20
30	Part 6	Section A	7	2	20
31	Part 6	Section A	10	3	30

(out of 118) were not precisely read in more than 3 times (representing more than 10% of the total number of reads) as shown in Table 13.14. In fact, one questionnaire item (Question No. 1) in part 3, section E was not precisely read more than 5 times representing more than 14% of the total reads.

Out of the total of the 118 questionnaire items, 15 of them were not read

Table 13.13: Proportion of respondents in Norwegian (out of 7 respondents) who did not answer exact

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 1	Section A	7	2	29
2	Part 1	Section A	8	2	29
3	Part 4	Section A	1.A	2	29
4	Part 4	Section B	2.B	3	43
5	Part 4	Section B	3.B2	2	29
6	Part 4	Section B	4.K	2	29
7	Part 5	Section B	1.A	2	29
8	Part 5	Section B	3	3	43
9	Part 5	Section B	14	2	29
10	Part 5	Section B	16	2	29
11	Part 6	Section A	10	2	29

Table 13.14: Proportion of readers (out of 36 readers) who did not read exact in all the languages (English, Norwegian and Indonesian)

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 3	Section C	2.A	5	13.8
2	Part 3	Section C	2.B	4	11.1
3	Part 3	Section E	1	6	16.6
4	Part 5	Section A	1.A	4	11.1
5	Part 5	Section B	13	5	13.8

exactly to 2 or more respondents, representing over 14% of the non-exact reads as shown in Table 13.15.

13.6 Discussion of questionnaire design and pretesting methods

In strengthening security-conscious care behaviour among healthcare workers, a study was initiated to assess the security practice level in various hospitals in Norway, Indonesia, and Ghana. However, healthcare workers in these countries consist of heterogeneous user groups with varying information security responsibilities such as management level, end-users, and all user groups. The all user group primarily intersects both management and end-users. These groups of personnel have different knowledge gaps in terms of their understanding of information technology and information se-

Table 13.15: Proportion of readers (out of 10 readers) in English of which the reading of the questionnaire items were not exact

#	Part	Section	Question No.	Count (#)	Proportion (%)
1	Part 1	Section A	2	3	30
2	Part 3	Section B	1.B2	3	30
3	Part 3	Section C	2.K	2	20
4	Part 3	Section C	2.A	5	50
5	Part 3	Section C	2.B	4	40
6	Part 3	Section C	2.B2	4	30
7	Part 3	Section D	1	2	20
8	Part 3	Section E	1	6	60
9	Part 3	Section E	1a.B	2	20
10	Part 4	Section A	1.K	2	20
11	Part 5	Section A	1.A	4	40
12	Part 5	Section A	1.B	2	20
13	Part 5	Section B	3a	2	20
14	Part 5	Section b	3	4	40
15	Part 5	Section B	13	4	40

curity with varying responsibilities. For instance, the management group of these healthcare staff has a deeper understanding of information technology and security with higher responsibilities to developing policies and ensuring their implementations in healthcare systems. On the contrarily, other users such as doctors and nurses may also just have the basic knowledge of healthcare information technology systems (such as EHR) to enable them to use these systems for therapeutic functions. In developing a questionnaire for analyzing the security practice of healthcare workers in a hospital which consists of all these user categories, there is hence the need to scale down the understanding of the questionnaire to meet all these user categories. Having pretested our questionnaire, this section discusses the findings in this study.

13.6.1 Principal findings

According to Hamed et al and Somekh et al., a quality questionnaire should be clear, unambiguous, and simple [62, 60]. Additionally, questionnaire designers are to avoid asking more than one question in a single question and should not use negative and double negatives. Furthermore, a quality questionnaire should adopt the usage of mutually exclusive questions and avoid questions that may irritate respondents[62, 60]. These can be achieved if the right methods are used in the design and pretesting stages of the questionnaire development. In this regard, questionnaire design and pretesting

methods were explored and used in designing and pretesting for the questionnaire that is intended to be used for analyzing healthcare security practice. In brief, the identified methods for designing questionnaire includes a rational method, prototypical, facet, construct, internal and external methods [47, 2, 67, 46, 32, 31, 35, 34, 9, 11, 64, 42, 6, 23] as shown in Table 13.1 and Table 13.2. Additionally, the identified pretesting methods include a the conventional, cognitive interview, behaviour coding, debriefing, response latency, vignettes, focus group and expert reviews [51, 8, 43, 12, 58, 18, 13, 69, 27, 45, 65, 17, 52, 50, 40, 70, 28] method as shown in Table 13.17. These methods were assessed in this study, towards designing and pretesting questionnaires for healthcare security practice analysis modelling and incentivization (HSPAMI)[73, 72, 71]. On conventional pretesting approach, various issues of the questionnaire were identified including complex terms (23%), incomplete response option(19%), unclear items(19%) and inappropriate scale arrangement (19%). With regards to behaviour coding method, issues relating to the readers and the interviewers were reported. From a total of 4,248, 92.35% responded with adequate answers in the English, Norwegian and Indonesian versions of the questionnaire. This finding is welcoming but further assessment on each questionnaire item was needed. if 15% or more responses are non-paradigmatic, then those items needed to be fixed. In the further assessment, 14 items had over 15% of responses with the need for clarification (see in table 13.7), 17 items were not responded with exact as shown in table 13.8 in all the languages (English, Norwegian and Indonesia). Furthermore, 10 items, 11 items and 31 items were not answered exact (with a significance of 15% or more) in the separate languages of the questionnaires in Indonesian, Norwegian and English respectively as shown in table 13.11,13.13 and 13.12. So, had it not been this tests, the respondents would have answered the questionnaire with these short-comings. This could have compromised the study results since the respondents might have provided wrong answers.

13.6.2 Assessment of questionnaire design and pretesting methods

This section assesses both the questionnaire design and pretesting methods having explored their objectives, pros and cons.

13.6.2.1 Selection and adoption of the questionnaire design methods

In answering the first research question (Q1), the questionnaire design methods which were selected and adopted in this study are the rational, prototypical, facet, and internal methods as shown in Table 13.16.

HSPAMI consists of multifaceted areas in the modelling and analyzing healthcare staffs' security practice as outlined below:

- Psychological influence on healthcare staff
- Social influence among healthcare staff
- Individual and organizational cultural effect
- Work demographic effect on healthcare staff security practice
- Social demographic influence on healthcare staff
- Healthcare staff security awareness and training

Additionally, there are various existing questionnaires for surveying for security practice in healthcare [26, 44, 3] but which questionnaire design methods are suitable for adopting existing items? Moreover, the KAB (Knowledge, Attitude, and Behavior) approach [3, 48] has been recommended to be used in the development of questionnaires in information security practice. This is because knowledge influences attitude and behavior and these need to be assessed with the information security practices. As explained in table 13.16, the prototypical, facet, construct and internal methods were found to be mutually exclusively useful and were hence combined in designing the questionnaire. Considering the rational method, a questionnaire that is designed with this method is incorporated with only the subjective view of the questionnaire developer. Therefore, a questionnaire that is assessed with the rational method alone can be suitable for exploration towards further studies but might not be effective enough for empirical studies for decision making such as incentivization measures, which is aimed towards improving security practice in healthcare. So the rational method was considered in the questionnaire design together with other methods in designing the questionnaire for HSPAMI. The rational method was used in separating questionnaire items into a section known as general security and privacy practice. From the perspective of the designers, this section was not related to any of the constructs as shown in Appendix 1.

The prototypical method is known to improve cognitive processing and stimulate a better understanding of the questionnaire items[47, 46]. This is so since the organization of the questionnaire items is always categorized based on the items that are more prototypical to each other. The prototypical approach relies on informal (knowledge based on rules of thumb or tricks of the trade) or tacit knowledge (eg., knowledge based on experience or job training) [46, 47, 67, 6, 23]. It is, therefore, suitable for the specification of implicit ideas and analyzing complex concepts[46]. The construction procedures are more elaborated in the prototypical method, than the rational method, and have therefore been considered as an effective method[46, 6], particularly for existing questions. The prototypical method was therefore used to select relevant existing questionnaire items into various constructs of the HSPAMI study questionnaire. This was necessary since the existing

questionnaire items were already tested and were needing modifications to fit into the various constructs of the study[48, 7].

The facet method has been considered to be important in identifying comprehensive questionnaire items to cover all areas of the constructs but it only relies on formal knowledge of the construct [46]. This happened to suit well with the nomological framework of our study as shown in figure 1.

The facet method is related to the construct method in the sense that, both of them rely on formal knowledge [47, 46] But the construct method requires theoretical and formal knowledge which can be used to develop a nomological network for empirical testing of hypothesis [46].

The method which seeks to address issues of internal validity is the internal method and it is suitable to be used for improving on an existing questionnaire. However, the specification and judgment of the items on the questionnaire are limited in scope because the method uses a statistical approach and not a theoretical framework that has the tendency to relate with a wider scope of variables. With regards to the external method, much as the wider scope of the study area can be covered, the idea of heterogeneous content has introduced complexity in using the method.

13.6.2.2 Assessment of pretesting methods

In providing answers to the second research question (Q2), conventional pretesting and behaviour coding were selected and used for the pretesting of the questionnaire. Conventional pretesting is a faster process of questionnaire evaluation. So this method was used to have a quick idea of whether our questionnaire had issues. However, conventional pretesting is unable to identify all questionnaire problems since respondents can wrongly answer the test questions based on their wrong interpretation of the questions. Conventional pretesting alone is not able to identify many pretesting problems because some kind of problems cannot be observed from the responses of the respondents, especially if the respondent themselves are not aware of the problems [51]. In a scenario where the respondent is not aware of the intention of a closed question, the person may miss-interprets the understanding of a closed question without leaving any sign of such behaviour. Additionally, in a conventional pretesting approach, the fieldworker or interviewer is exposed to the intention of the pretesting exercise. Whereas the intention of the pretesting may remain undisclosed to the respondents. So the respondents are mostly not able to ask relevant questions that meet the intent of the question, unlike the interviewer who has the privilege of knowing that [51, 12]. Fortunately, these gaps can be covered by complementing with any of other pretesting methods such as cognitive interview, behaviour coding, debriefing, response latency, vignettes, experimental method, focus group, or expert review methods[51].

Vignettes involve multiple testing which enables an interviewer to have a comprehensive view of the question problem. It also combines the strength of both internal and external validity but the vignette is considered artificial because it adopts hypothetical behaviour. However, hypothetical behaviour in an experiment may not reflect the behaviour of one's real life [25]. The experimental approach has also been considered to be easy to implement but it greatly relies on the assumed module and lacks effective evaluation methods [50]. In a focus group, the thought process can be stimulated by the comments of others. The members' reaction and their comments can provide valuable ideas to help in revising the questionnaire items [57]. However, the results are difficult to implement and it also takes a lot of time to organize and process the results and in the end, very few terms, topics, or issues are addressed [13].

In view of these, behaviour coding was combined with the conventional pretesting in this study. Behaviour coding pin-points to the problem of the questionnaire item rather than providing the causes as compared to other pretesting methods such as cognitive interviewing, vignettes, debriefing, and focus groups [16] as listed in Table 13.17 . Notwithstanding, behaviouur coding results are more reliable since the data are collected in a situation that reflects the main study. Furthermore, whereas other pretesting methods such as cognitive interviewing, may report pseudo-problems in order to just please the interviewer, respondents of behavior coding report the real problems. Moreover, behavior coding is more objective, reliable, easy to do and it provides data under realistic conditions [29]. Behavior coding is also a comparatively simpler and low-cost method[16, 13].

As a result, the designed questionnaire was sent to respondents in Norway, Indonesia, and Ghana. The target group was healthcare staff who use information systems in providing healthcare services to patients in the hospitals. The pretesting methods were conducted with various types of respondents in healthcare including nurses, doctors, IT researchers in healthcare, and laboratory personnel who were working in hospitals that were not part of the main study healthcare facilities. Conventional pretesting questionnaire in English was first sent out to the target respondents in various hospitals in Ghana and Norway and having independently obtained ethical clearance from the research councils of these countries. Subsequently, invitations were sent out to healthcare workers in these countries to help in testing our questionnaire using the behaviour coding method. Respondents were motivated to participate by refunding each of them an amount of GHS 10.00 for using their internet data. A synergy of these methods was used to develop and pretest the questionnaire for healthcare security practice.

13.6.3 Pretesting of questionnaire

To determine if our questionnaire for collecting healthcare staff security practice was reasonably understandable by the multifaceted respondents as specified in our hypothesis (H1), conventional pretesting and behaviour coding methods were used to pretest the questionnaire.

13.6.3.1 conventional approach

A number of issues were identified when the questionnaire was pretested with conventional pretesting and behaviour coding. With conventional pretesting, the respondents identified various problems that were associated with the questionnaire including issues relating to questions scale arrangement (19%), incomplete response options(19%) , lack of understanding of the structure of information systems of respondents, use of undefined abbreviations, unrelated questions to respondents, unclear(19%) and complex questions(19%), the insignificant difference between questions, grammatical and spelling mistakes and security and privacy concerns of respondents, as shown in table 13.4. This failed to agree with the hypothesis that the questionnaire was without issues.

For example, in a questionnaire item such as, "It is inconvenient to my work for me to use strong password policies such as multi-factor authentication, long password characters mixed with alphabets, numbers, and characters", it was realized that IT personnel in healthcare had no problem with understanding of the term multi-factor authentication. However, ordinary users of healthcare information systems including nurses, doctors, and healthcare administrators, who do not have technical skills in IT, could not comprehend the meaning of "multi-factor authentication". So in the repair of this question, an explanation of the term was provided. Additionally, as shown in Figure 13.1, a respondent indicated some of the questions which were unclear (19%), and further indicated the exclusion of some of the roles in the laboratory department.

Related studies including Developing a Security Behavior Intentions Scale (SeBIS) and human aspect of information security questionnaire(HAIS-Q) were much focused on improving the effectiveness of surveys relating to information security. However, a number of shortfalls were observed. First of all, their target respondents did not consider comprehensive respondents of various roles and activities in an organizational setting like healthcare. Therefore, roles such as IT personnel who perform IT administrative duties including backups and updates were excluded. Additionally, though HAIS-Q used some pretesting methods, other pretesting methods were not assessed. Additionally, unlike this paper, the studies did not fully consider comprehensive questionnaire design methods.

13.6.4 Behavior coding responses

In the behavior coding exercise, 50 questionnaire items out of the 118 were remarked to have issues as shown in Table 13.18. Additionally, all the non-paradigmatic responses in this study (interruption, clarification, qualification and don't know) except the refusal to answer reported various questionnaire items to have issues as shown in Table 13.5, Table 13.6, Table 13.7, Table 13.8, Table 13.9, and Table 13.10. The hypothesis(H1) is not paradigmatic and the questionnaire would have been administered with these problems despite having pretested it with the conventional method. In the conventional pretesting, the respondents answered these questionnaires based on their subjective understanding. Even if they had issues with any of the questionnaire items, the respondents in the conventional pretesting were not subjected to prop for clarifications prior to responding to each of the items and therefore answered the questions in their way of understanding. The behaviour coding has effectively solved this gap by providing the respondents with the opportunity to inquire if they have any issues with any of the questionnaire items.

Much as the behaviour coding indicated the issues pertaining to various questionnaire items, there have been suggestions that when 15% or more of the responses to the questionnaire items are non-paradigmatic, it is an indication that there are significant issues with that questionnaire item [45, 13]. On that note, questionnaire items in Table 13.7and Table 13.8 definitely needed significant repairs.

Furthermore, since the study was conducted in three languages, (English, Norwegian and Indonesian Language) translation errors in the questionnaire could not be overlooked. So the analysis of the responses in these languages also showed various errors in the questionnaire items. Table 13.11, Table13.12, and 13.13respectively showed all the questionnaire items in Indonesian, English and Norwegian languages which significantly require repairs. The English language version showed more of its questionnaire items (31) that need repairs as compared to Indonesian(10) and Norwegian (11), suggesting that the English version comparatively had more issues with its questionnaire items.

As behaviour coding, merely pinpoints the questionnaire items that have issues without providing their causes [29, 16], we augmented the behaviour coding method by providing opportunities for respondents and interviewers to comment or indicate the cause of problems with each of the questionnaire items. A total of 50 questionnaire items out of the 118 attracted comments indicating various causes of the questionnaire item problems. This adjustment of the behaviour coding strengthened the study and improved the quality of the questionnaire pretesting.

The behaviour coding was adopted with the ultimate aim to pretest the questionnaire. So the interviewer's reading behaviour was captured to be

analyzed towards improving on the questionnaire. Some attempts have related the behaviour codes to certain problems[45, 13]. Questionnaire items that are not exactly read as worded have been phrased in an awkward way. Sometimes those items could also be having words that are difficult to pronounce. Also, questionnaire items that are frequently responded to with interruptions tend to provide infirm explanations at their conclusion. Additionally, responses to questionnaire items having sorted for clarification imply that the questionnaire item does not fit the respondents' experience or frame of reference and is often vague or contains a poorly defined term or concept. Whilst questionnaire items that are responded to with inadequate answers often require a level of details the respondents are not capable of providing.

13.7 Conclusions

While healthcare organizations are mandated to collect detailed sensitive personal health information for the purpose of correct patient identification and effective therapeutic measures, data breaches have become rampant with the potential to jeopardize effective healthcare. The adversaries usually gain access to the healthcare data through the human elements including the healthcare staff who have legitimate access to the healthcare records. To curtail this, research is being conducted using a questionnaire to determine the gaps between required security practice and current security practices in healthcare. The challenges of healthcare staff in complying with the security requirement would also be determined towards resolving any identified dilemmas. With such high ambition, an effective questionnaire needs to be developed to meet the needs of the diverse respondents who have variant IT skills gaps, experiences, and roles. Therefore, questionnaire design and pretesting methods were identified in a literature survey and used in designing and pretesting the questionnaire for healthcare security practice analysis.

The identified questionnaire pretesting methods were rational, prototypical, facet, construct, internal and external methods. Additionally, the pretesting methods which were identified include a conventional, cognitive interview, behaviour coding, debriefing, response latency, vignettes, experimental, focus groups, and expert reviews.

The contribution in this study is in different facets. Firstly, different types of questionnaire pretesting methods were identified in the survey. Secondly, the pretesting methods were accessed based on their advantages for effective pretesting of questionnaires towards healthcare security practice. Finally, effective pretesting methods were used to pretest questionnaires for healthcare security practice.

In the pretesting of the questionnaire, various questionnaire issues were

identified to include issues with an arrangement of questions scales, lack of understanding of healthcare information systems' structure of all hospitals, unclear questions, the insignificant difference between questions, issues of security and privacy of respondents, problematic questions, inadequate questions, and complex terms. These issues were identified, having combined the conventional pretesting method with cognitive interview and behaviour coding. All the identified issues are pitfalls to watch when developing a questionnaire to be responded to by an organization that is characterized by varying levels of IT skills. Even though the identified problems have been corrected based on inputs from the study respondents and focus group experts, further works including animated and cartoonist questionnaire is to be explored in future studies. If a question in the questionnaire item mentions a term such as a "URL" or a "multi-factor authentication", an animated image or cartoon will be used to provide a better understanding of such wording.

13.8 Appendices

13.8.1 A sample responses from conventional pretesting

Dear Sir,

Kindly find below my comment on your questionnaire.

1. I spent 12 minutes

2. Question 2 did not capture the entity of the Laboratory profession since its categorised just like the nurse and nurse assistant
i. Laboratory Assistant
ii. Clinical Laboratory Technician
iii. Clinical Laboratory Scientist

3. Question 5 appears unclear.
i. Is it my understanding of what it entails?
ii. Or do you mean my understanding of the reasons behind such policies?

4. Despite the fact I appreciate sentences with negations to mean positive as in the cases of question 62 and 64, so many people struggle with such and might give answers that might not really truly reflect their intentions hence compromising your research.

Figure 13.2: Sample respond from a respondent in the pretesting study.

13.9 Bibliography

[1] AMELANG, M., HERBOTH, G., AND OEFNER, I. A. prototype strategy for the construction of a creativity scale. *European Journal of Personality-*

Sep; 5, 4 (1991), 261–85. 369

[2] AND, S. L. C. and modern methods of psychological scale construction. *Social and Personality Psychology CompassJan; 2*, 1 (2008), 414–33. 365, 385

[3] ANWAR, M., ET AL. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. 386, 399

[4] BEATTY, P. C., AND WILLIS, G. B. Research synthesis: The practice of cognitive interviewing. *Public opinion quarterly 71*, 2 (2007), 287–311. 400

[5] BOX, D., AND POTTAS, D. Improving information security behaviour in the healthcare context. *Procedia Technology 9*, 2013 (2013), 1093–1103. 362

[6] BROUGHTON, R. A. prototype strategy for construction of personality scales. *Journal of Personality and Social PsychologyDec; 47*, 6 (Dec 1984), 13–34. 365, 385, 386

[7] CALDWELL, A. H.-Q. A. smart solution to cyber security2017-08-30; Available from:, 2017. Available from: `https://www.dst.defence.gov.au/podcast/hais-q-smart-solution-cyber-security`. 387, 399

[8] CANNELL, C. F., AND RL., K. The collection of data by interviewing. *Research methods in the behavioral sciences* (1953), 327–80. 371, 385

[9] CATTELL, R. B., SAUNDERS, D. R., AND STICE, G. *Handbook for the sixteen personality factor questionnaire. 1957.* IPAT, F. test forms A, B, and C. Champaign, IL, 1957. 366, 385

[10] CLARK, E. V., AND WHAT'S, I. N. A. What's in a word? on the child's acquisition of semantics in his first language11. *ON THE CHILD'S ACQUISITION OF SEMANTICS IN HIS FIRST LANGUAGE 11* (1973), 65–110. Available from: `https://doi.org/10.1016/B978-0-12-505850-6.50009-8`. 366

[11] COMREY, A. L. . Factor-analytic methods of scale development in personality and clinical psychology. *Journal of Consulting and Clinical Psychology 56* (1988), 754–761. 366, 385

[12] CONVERSE, J. M., JEAN MCDONNELL, C., AND QUESTIONS, P. S. S. *Handcrafting the standardized questionnaire*. Sage;, 1986. 371, 385, 387

[13] CZAJA, R. Questionnaire pretesting comes of age. *Marketing Bulletin-Department of Marketing Massey UniversityMay; 9* (1998), 52–66. xix, 371, 372, 374, 385, 388, 390, 391, 400

[14] DE JONG PF. An application of the prototype scale construction strategy to the assessment of student motivation. *Journal of personalitySep; 56*, 3 (1988), 487–508. 369

[15] DESIGN AND, B. W. T. *and understanding of survey questions*. Lexington Books;, 1981. 372

[16] DIJKSTRA, W. Behavior coding. In *Using behavioral coding to identify cognitive problems with survey questionsh (p* (Inc, 2011), Sage Publications, pp. 54–55). 388, 390

[17] DRAISMA, S., AND LATENCY AND, D. W. R. linguistic expressions as indicators of response error. methods for testing and evaluating survey questionnaires. *Methods for testing and evaluating survey questionnairesJun 25*, 13 (JUN 2004), 131–147. 374, 385

[18] DRENNAN, J. Cognitive interviewing: verbal data in the design and pretesting of questionnaires. *Journal of advanced nursing 42*, 1 (2003), 57–63. 371, 372, 385

[19] DRYE, S., AND A. SALAM, A. framework for health care information assurance policy and compliance. *Commun. ACM 53* (2010), 126–131. 361

[20] DRYE, S., AND A. SALAM, A. framework for health care information assurance policy and compliance. *Commun. ACM 53* (2010), 126–131. 362

[21] EDELEN, M. O., AND BB., R. Applying item response theory (irt) modeling to questionnaire development, evaluation, and refinement. *Quality of life researchAug 1*, 16 (Aug 2007), 5. 375

[22] EDWARDS, A. L. The measurement of personality traits by scales and inventories. 1970. 369

[23] EH., R. On the internal structure of perceptual and semantic categories. In *Cognitive development and acquisition of languageJan 1* (1973), pp. 111–144. 365, 385, 386

[24] EHRENFELD, J. M. Wannacry, cybersecurity and health information technology: A time to act. *Journal of medical systems 41* (2017), 7. 362

[25] EVANS, S. C., ROBERTS, M. C., KEELEY, J. W., BLOSSOM, J. B., AMARO, C. M., GARCIA, A. M., STOUGH, C. O., CANTER, K. S., ROBLES, R., AND GM., R. Vignette methodologies for studying clinicians decision-making: Validity, utility, and application in icd-11 field studies. *International journal of clinical and health psychologyMay 1*, 15 (2015), 2. 388

[26] FERNANDEZ-ALEMAN, J. L., SANCHEZ-HENAREJOS, A., TOVAL, A., SANCHEZ-GARCIA, A. B., HERNANDEZ-HERNANDEZ, I., AND FERNANDEZ-LUQUE, L. Analysis of health professional security behaviors in a real clinical setting: an empirical study. *Int J Med Inform 84*, 6 (2015), 454–467. 386, 399

[27] FORSYTH, B., ROTHGEB, J. M., AND GB., W. Does pretesting make a difference? an experimental test. *Methods for testing and evaluating survey questionnairesJun 25* (2004), 525–46. 372, 373, 385

[28] FORSYTH, B. H., AND LESSLER, J. L. Cognitive laboratory methods: A taxonomy. In *Measurement Errors in Surveys*, P. Biemer, R. Groves, L. Lyberg, and a. S. S. N. Mathiowetz, Eds. John Wiley,, New York, 1991, pp. 393–418. 375, 385

[29] FOWLER, JR., F. J., AND CANNELL, C. F. Using behavioral coding to identify cognitive problems with survey questions. In *Answering questions: Methodology for determining cognitive and communicative processes in survey research (p* (Jossey-Bass/, 1996), N. Schwarz and S. Sudman, Eds., Wiley, pp. 15–36. 388, 390

[30] GOSLING, S. D., RENTFROW, P. J., SWANN, J. R., AND WILLIAM, B. A. very brief measure of the big-five personality domains. *Journal of Research in personality 37*, 6 (2003), 504–528. 399

[31] GUTTMAN, L. *Introduction to facet design and analysis'*. in proceeding the Fifteenth international congress of psychology. 366, 385

[32] GUTTMAN, L. An outline of some new methodology for social research. *Public Opinion QuarterlyJan 1*, 18 (1954), 4. 366, 385

[33] HEALTHITSECURITY. Cybersecurity best practices for data security. @SecurityHIT, 2017. 362

[34] JACKSON, D. N. The dynamics of structured personality tests. *Psychological Review 78*, 3 (1971), 229. 365, 366, 385

[35] JACKSON, D. N. S. P. A. In b. In *Handbook of general psychology (pp*, B. Wolman, Ed. Prentice Hall, Englewood Cliffs, NJ, 1973, pp. 775–792. 365, 366, 385

[36] JD., B. What is construct validity. Available at(accessed 10 June 2020), 2013. Available from: `https://jalt.org/test/bro_8.htm`. 370, 371

[37] KAPLAN, R. M., BUSH, J. W., AND STATUS, B. C. H. Health status: types of validity and the index of well-being. *Health services research 11*, 4 (1976), 478. 370, 371

[38] KAZI, A. M., AND DESIGNING AND, K. W. Q. validation. *Journal of the Pakistan Medical Association 62*, 5 (2012), 514. 365, 370

[39] KL., G. *Using cognitive testing in the design of a business survey questionnaire*. Inpresentation at the annual meeting of the American Association for Public Opinion Research, Salt Lake City, UTMay, 1996. 372

[40] KRUEGER RA. FOCUS GROUPS:, A. practical guide for applied research. *Sage publications;Aug 14* (2014). 375, 385

[41] MARTIN, E., SCHECHTER, S., AND TUCKER, C. Interagency collaboration among the cognitive laboratories: past efforts and future opportunities. Working Paper 28, Statistical Policy, 1998. 371

[42] MEEHL, P. E. The dynamics of structured personality tests. *Journal of Clinical Psychology 1*, 4 (1967), 517–522. 367, 385

[43] MOSER, C. A., AND KALTON, G. *Survey methods in social investigation*. Routledge, ;Mar 2, 2017. 371, 385

[44] NG, B. Y., KANKANHALLI, A., AND YC., X. Studying users' computer security behavior: A health belief perspective. *Decision Support SystemsMar 1*, 46 (2009), 4. 386

[45] OKSENBERG, L., AND KALTON, G. New strategies for pretesting survey questions. *Journal of official statisticsSep 7*, 3 (1991), 349–365. 373, 385, 390, 391

[46] OOSTERVELD, P., ET AL. *Questionnaire design methods*. Berkhout Nijmegen BV, 1996. 362, 365, 366, 367, 385, 386, 387

[47] OOSTERVELD, P., VORST, H. C., AND SMITS, N. Methods for questionnaire design: a taxonomy linking procedures to test goals. *Quality of Life ResearchSep 15*, 28 (2019), 9. 362, 365, 366, 367, 385, 386, 387

[48] PARSONS, K. et al., the human aspects of information security questionnaire (hais-q): Two further validation studies. *Computers & Security 66* (2017), 40–51. 386, 387, 399

[49] PEDERSEN, S., AND HARTVIGSEN, G. Lessons learned from 25 years with telemedicine in northern norway. 2015. *Lessons learned from 25* (2015). 361

[50] PP., B. Modeling measurement error to identify flawed questions. *Methods for testing and evaluating survey questionnaires 25* (JUN 2004), 225–46. 375, 385, 388

[51] PRESSER, S., COUPER, M. P., LESSLER, J. T., MARTIN, E., MARTIN, J., ROTHGEB, J. M., AND SINGER, E. Methods for testing and evaluating survey questions. *Public opinion quarterlyMar 1*, 68 (2004), 1. 371, 372, 373, 374, 375, 385, 387, 400

[52] PRETESTING METHODS: COGNITIVE INTERVIEWS, H. K. C. respondent debriefing, and behavior coding. *Survey Methodology 2* (2004), 1–20. 371, 374, 385

[53] RB., R. Tips for developing and testing questionnaires/instruments. *Journal of extensionFeb; 45*, 1 (2007), 1–4. 365, 369, 370

[54] REEVE, B. B., AND LC., M. Item response theory modeling for questionnaire evaluation. *Methods for testing and evaluating survey questionnairesJun 25*, 1 (2004), 247–74. 375

[55] ROSCH, E. H. Principles of categorization. In *Cognition and categorization (pp*, E. H. Rosch and D. B. Lloyd, Eds. Erlbaum, Hillsdale, NJ, 1978, pp. 27–48. 366

[56] ROYSTON, P., AND BERCINI, D. Questionnaire design research in a laboratory setting: results of testing cancer risk factor questions. In *In1987 Proceedings of the Section on Survey Research Methods* (1987), pp. 829–33. 372

[57] ROYSTON, P., AND BERCINI, D. Questionnaire design research in a laboratory setting: results of testing cancer risk factor questions. In *In1987 Proceedings of the Section on Survey Research Methods* (1987), pp. 829–33. 388

[58] SCHECHTER, S., BEATTY, P., AND A., B. Cognitive issues and methodological implications in the development and testing of a traffic safety questionnaire. In *InProceedings of the Survey Research Methods Section of the American Statistical Association* (1994), pp. 1215–1219. 371, 372, 385

[59] SCHUWIRTH, L. W., AND VERHEGGEN, M. M. Van der vleuten cp, boshuizen hp, dinant gj. *Do short cases elicit different thinking processes than factual knowledge questions do?. Medical EducationApr 22*, 35 (2001), 4. 372

[60] SOMEKH, B., AND LEWIN, C. *Theory and methods in social research*. Sage, 2011. 384

[61] STOUTHARD, M. E., MELLENBERGH, G. J., AND HOOGSTRATEN, J. Assessment of dental anxiety: a facet approach. *Anxiety, Stress and CopingJan 1*, 6 (1993), 2. 366

[62] TAHERDOOST, H. How to design and create an effective survey/questionnaire; a step by step guide. *International Journal of Academic Research in Management (IJARM) 5*, 4 (2016), 37–41. 384

[63] TAYLOR, C. Clinical problem?solving in nursing: insights from the literature. *Journal of Advanced NursingApr; 31*, 4 (2000), 842–9. 372

[64] THURSTONE, L. L. Multiple factor analysis. *Psychological Review 38* (1931), 406–427. 366, 385

[65] VAN DER ZOUWEN, J., AND JH., S. Evaluating survey questions by analyzing patterns of behavior codes and question-answer sequences: A diagnostic approach. *Methods for testing and evaluating survey questionnairesJun 25* (2004), 109–30. 373, 385

[66] VERISON. *2019 Data breaches report*. 2019. Available from: `https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf`. 362

[67] WALLER, N. G., DEYOUNG, C. G., AND TJ., B. J. The recaptured scale technique: A method for testing the structural robustness of personality scales. *Multivariate behavioral researchJul 3*, 51 (2016), 4. 365, 385, 386

[68] WILLIAMS, P. A. In a trusting environment, everyone is responsible for information security. *Information Security Technical Report 13*, 4 (2008), 207–215. 362

[69] WILLIS, G., DEMAIO, T., AND HARRIS-KOJETIN, B. Cognition and survey research. *wILLY* (1999), 133–53. 372, 375, 385

[70] YAN, T., KREUTER, F., AND SURVEY QUESTIONS: A COMPARISON OF METHODS, T. R. E. *Journal of Official StatisticsDec 1*, 28 (2012), 4. 375, 385, 400

[71] YENG, K., P., B. Y., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: A literature survey. In *Studies in health technology and informatics 261: p* (2019), pp. 239–245. 362, 365, 385

[72] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *in 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), IEEE. 362, 385

[73] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *IEEE International Conf* (2019), IEEE. 362, 365, 385

Table 13.16: Questionnaire design methods used for designing questionnaire in healthcare security practice

Method	How it was used in HSPAMI	Example
Prototypical	From Figure 1, both independent and mediating variables have different categories. This method was used to present questionnaire items based on all the categories, to enhance cognitive processing.	As shown in figure 1, the questionnaire items will be categorized into the various constructs of the nomological diagram such as psychological, social and cultural and demographic variables such that the item within each category are related but differ in various categories.
The facet method	This method was adopted due to its objective to adequately represent the questionnaire items to meet the content validity in a systematic manner.	With reference to the questionnaire in appendix 1, each construct is further categorised. For instance, in the social construct, sub-construct were identified to include Formal control and informal controls of which questionnaire items were developed for each of these constructs towards enhancing the content validity of the questionnaire
The Construct	The entire psycho-socio-cultural aspect of the HSPAMI study is based on a theoretical background as shown in figure 1, where psychological, social, cultural theories have been combined to form individual traits. The construct method was adopted in the design so that the questionnaire outcome will be able to adequately assess each of the constructs	An instance is the construction of the questionnaire to consider all the constructs (independent variables) as shown in figure 1
Internal method	The method was used in developing questionnaire based on existing questionnaires since the method focuses on empirical relations between questionnaire items and is mostly used for developing questionnaires based on existing questionnaire items	From appendix 1, existing questionnaire items that are related to the various mediating variables (security practices) were selected from [26, 3, 48, 7, 30]

Table 13.17: Pretesting techniques and their objectives

Method	Objective
Conventional pretesting	To obtain a subjective evaluation of the questionnaire from the answered results of respondents
Cognitive interview	Focuses on understanding the process of answering the questionnaire in order to evaluate the understanding of the objective of the questionnaire
Behaviour coding	A third person observes the interaction between the interviewer and the participant to identify signs of misunderstanding or difficulties based on the occupancy frequencies towards improving upon the identified items [13, 4]
Debriefing	Much like probes, the objective is to determine comprehensiveness and problems associated with the questionnaire item[13, 4]
Response latency	To identify difficult or complex questions through delays of respondents which are correlated with their uncertainties
Vignettes	Assesses how respondents understand concepts in different wording scenarios, questions and wording problems in relation to the goal of the study [51, 13]
Experimental	Aim to determine errors in the questionnaire by repeatedly asking the same respondents, to answer a questionnaire at a given number of times and the results analysed
Focus groups	Assesses the way respondents understand keywords, terms and phrases
Expert reviews	Designed questionnaires are reviewed by experts for possible problems [70]

Table 13.18: Comments from behaviour coding

#	Part	Section	Question No.	Comments
1	Part 1	Sect A	1	What is your gender(add others)
2	Part 1	Sect A	2	Typo, personnel
3	Part 1	Sect A	7	Had formal training on i formation security ;Knows they have a policy but have not been trained;Respondent doesnt work in the hospital as a healthcare professional
4	Part 1	Sect B	8	Whant kind of brak?
5	Part 1	Sect B	10	specific on often
6	Part 2	Sect A	10	Complex question; Start with During emergency situation
7	Part 3	Sect A	1.K	is it about me in particula
8	Part 3	Sect B	1.K	can be harmful
9	Part 3	Sect B	1.B	update to social instead;THEIR NETWORK DOESNT ALLOW THAT
10	Part 3	Sect B	1.B2	Find out about security practice first before asking question. Put training aspect to it
11	Part 3	Sect C	1.K	Indicate Where;How to incoporate "i DONT KNOW". 3; Condition if user recieves alert messages or not options;Indicate where yes,no, cant remember or dont know
12	Part 3	Sect C	1.B2	typo
13	Part 3	Sect C	2.K	policy or etc; typo
14	Part 3	Sect C	2.A	Remove s from link
15	Part 3	Sect D	1	Restarts machine when instructed by the leader
16	Part 3	Sect E	1	incomplete caption, Typos; Work colleagues?
17	Part 3	Sect E	1a.K	Getting second opinion from colleague on results should be a problem however, sharing patient information to colleagues is bad
18	Part 3	Sect E	1a.B	From seeing instead
19	Part 4	Sect A	1.A	choices are confusing
20	Part 4	Sect A	1.B2	not applicable to her
21	Part 4	Sect A	2.K	Add patients information. Question is too general
22	Part 4	Sect A	2.B	what is anything
23	Part 4	Sect A	2.B2	change dont to did not, OR didn't
24	Part 4	Sect A	3.K	punished by who?
25	Part 4	Sect A	3.A	Type of action taken(we need to specify if I leave somebody will access my data)
26	Part 4	Sect A	3.B	Giving your password to a friend to view patient data : can be considered
27	Part 4	Sect B	1.A	Choices are confusing
28	Part 4	Sect B	1.B2	Not applicable
29	Part 4	Sect B	2.K	Clarrification;Require "not applicable"
30	Part 4	Sect B	2.B	Not application
31	Part 4	Sect B	3.B2	Not applicable
32	Part 4	Sect B	4.B	What is a shared password?
33	Part 4	Sect B	5.A	Not applicable
34	Part 4	Sect B	5.B	how do you dispose the sensitive
35	Part 4	Sect B	5.B2	Many typos;Not applicable
36	Part 5	Sect A	1.A	Typos (Spelling error: Thrust, sase)
37	Part 5	Sect A	3a	use check box;Should ask this earlier;.had formal training
38	Part 5	Sect B	3	Remove if
39	Part 5	Sect B	4	Introduce Which,; management team; Not all the time
40	Part 5	Sect B	6	use "someone"
41	Part 5	Sect B	8	personal mobile, add some example
42	Part 5	Sect B	9	Qualified answer
43	Part 5	Sect B	10	Temporal -check;what is sikkerhetstiltak'
44	Part 5	Sect B	13	Remove if
45	Part 5	Sect B	14	which media
46	Part 5	Sect B	16	Not clear question
47	Part 6	Sect A	3	clarify dependable
48	Part 6	Sect A	6	contradicts extrovert
49	Part 6	Sect A	9	Clarify calm
50	Part 6	Sect A	10	Clarify conventional;Use a different word for 'konvensjonal'

Chapter 14

A comprehensive assessment of human factors in cyber security compliance towards enhancing the security practice of healthcare staff in paperless hospitals

Prosper Kandabongee Yeng ; Muhammad Ali Fauzi ; Bian Yang

Abstract

Recent reports indicate that over 85% of data breaches are still caused by a human element, of which healthcare is one of the organizations that cyber criminals target. As healthcare IT infrastructure is characterized with a human element, this study comprehensively examined the effect of psycho-social-cultural and work factors on security behaviour in a typical hospital. A quantitative approach was adopted where we collected responses from 212 healthcare staff through an online questionnaire survey. A broad range of constructs was selected from psychological, social, cultural perception, and work factors based on earlier review work. These were related with some security practices, to assess the information security (IS) knowledge, attitude and behaviour gaps among healthcare staff in a comprehensive way. The study revealed that work emergency (WE) has a positive correlation with IS concious care behaviour (ISCCB) risk. Conscientiousness also had a positive correlation with ISCCB risk , but agreeableness was negatively correlated with information security knowledge (ISK) risk , and information security attitude (ISA) risk. Based on these findings, intrinsic and extrinsic motivation methods combined with cutting-edge technologies can be explored to discourage IS risks behaviours while enhancing conscious care security practice.

14.1 Introduction

Paperless or folder-less system is a common term used to denote the adoption of full electronic health records (EHR) systems used by hospitals in

Ghana. In paperless systems, the hospitals do not use hard copy papers or folders to document and store patient care processes. Instead, all the patient activities at the healthcare facility (such as OPD visits, medical investigations, diagnosis and treatments, inpatient and outpatient documentation, referrals, and ordering of tests) are carried out in the EHR system [58, 78]. The benefits of paperless systems cannot be overemphasised as the systems improve the efficient management of patients' information, reduce physical storage space for medical records, and improve clinical decision support [45, 34, 17].

In hindsight, cyber security incidents remain a threat to the use of these information systems [74] of which healthcare systems are among the most targeted systems. Several reasons account for this. Firstly, information security solutions have traditionally been focused on technical measures such as firewall configurations, demilitarise zone, Intrusion detection and prevention systems, authentication, and authorisations in mitigating risks however, the human aspect of IS management (also called the human firewall) has received less attention as an important factor in mitigating security issues [23, 71]. Meanwhile, current dynamics in security issues cannot be resolved with only technical measures especially in an era where humans are considered the weakest link in the security chain [71, 48, 68]. Secondly, healthcare is most suitable for cyber criminals due to urgency requirement by healthcare staff to access patients records. For instance, in ransomware attack scenario, the healthcare, the authorities would be willing to pay for the ransoms for timely access of patients records.

There is a broad range of human factors that contribute to security violations in healthcare. These include psychological, social, cultural, work factors and individual factors [75]. Security researchers often investigate these factors towards enhancing security practices; however the assessments are not often comprehensively performed, leaving possible gaps of vulnerabilities in the human element. For instance, Anwar et al. investigated the significance of gender factors in security practice [7]. While this is essential, other variables, such as work factors, where not considered in the study. This means if findings in Anwar et al. were to be considered for enhancing security practice in a typical hospital, issues on individual difference in terms of gender among healthcare staff will be detected and resolved. However, issues relating to other factors of the human element will not be covered. This may still leave a security gap among the staff's security practice. This study contributed to bridging this gap having adopted a comprehensive approach where a broad range of factors, including psychological, social, cultural, individual, and work factors were assessed in a comprehensive way.

In view of the above, the objectives of this study include:

- To comprehensively assess the effect of individual factors and perceptions, including psychological, social, and cultural aspects on IS

knowledge, attitude and behaviour among healthcare staff.

- To examine the effect of work factors (such as workload and work emergency) on cyber-security knowledge, attitude, and the intended security conscious care behaviour (ISCCB) of healthcare workers.

- To assess the effect of cyber security knowledge and attitude on the intended security conscious care behaviour of healthcare staff.

Factors found to have significant risks on conscious care security practices can be discouraged with extrinsic motivation (motivations based on external factors, eg financial or punishment) [33, 18, 55] and intrinsic motivations (incentives that stem out of one's self) [51, 69] while promoting factors that have positive impact in IS security practice.

The remaining part of the paper is organised to include theoretical background and hypotheses. In this section, related theories that were used in similar studies have been reviewed. Subsequently, the theoretical model and hypotheses were developed. This section is followed by the study approach and the method section which explained how the study was conducted. The results were then described in the result section. Finally, the results were then discussed and concluded in the conclusion section.

14.2 Related work and theoretical background in security behaviour within healthcare

14.2.1 Related work

Healthcare staff plays a vital role in the space of information security as they are required to abide by end user security policies amidst their core duties [26, 73]. Failure to do so can lead to vulnerabilities that can be exploited to cause internal or external breaches. Therefore, in efforts to improve upon the staff's conscious care behaviour, it is imperative to identify and assess a broad range of factors that affect the staff's security behaviour to enable management to "push" the right incentive "buttons" towards improving conscious care security practices. Information security conscious care behaviour refers to the healthcare workers' active compliance with the information security policies and ethics in order to safeguard the confidentiality, integrity, and availability (CIA) of the organisational assets [56, 75]. Having conducted a study into security requirements [76], some compliance measures were identified and adopted in this work. These include internet use, email use, social media use, password management, incident reporting, information handling, and mobile computing. These measures were considered because they are more prone to security violations by the humans. [75, 48].

Prior to this empirical study, various reviews pointed out theory of plan behaviour (TPB), protection motivation theory (PMT), health belief model (HBM), social control (SC), technology acceptance model (TAM) and personality traits as some of the psychological, social, and cultural factors that are used to investigate information security practices [74, 75, 40]. While these studies presented knowledge on the overview of all the necessary theories for incentive factors, these methods were not practically assessed in a holistic fashion, but provided a foundation for empirical assessments. Fernandez-Aleman et al. evaluated the security practice of healthcare staff in an actual healthcare facility [22]. The study tried to cover this gap and the authors reviewed IS security governance tools such as standards, guidelines, and best practices and used this information to develop a questionnaire instrument. The instrument was then used to conduct a survey to which 180 healthcare staff responded . The study found weak passwords among 62.2% of the staff, half of the respondents failed to protect unauthorised access to patients information, and 57% did not know the procedure to report security violations. A related study also assessed healthcare staff security practices with a total of 554 completed questionnaires to understand the security behaviour of healthcare workers in a real hospital. The study also identified significant security gaps among the hospital staff, including the practice of sharing computers and passwords [5]. While these studies [22, 5] pointed out that the staff of the respective facilities needed both preventive and corrective measures to prevent them from causing security violations, the studies did not pinpoint the exact factors influencing this IS security misbehaviour.

Comprehensive factors need to be examined among healthcare workers in relation to their cyber security behaviour. That will give a sense of direction as to how to improve upon the ISCCB of the workers. To this end, Anwar et al. conducted a study to find out if gender differences play a role in cyber-security behaviour. Psychological and social factors of PMT and TPB were adopted as mediating variables [7]. The findings revealed that gender has a significant effect on SE, prior experience, and computer skills. This was also the right step towards a holistic approach however, other factors relating to knowledge and attitude towards IS security practice were not examined. Additionally, work factors such as workload, and work emergency in healthcare were not considered; meanwhile all these are important factors that can have a significant effect on IS conscious care behaviour[73, 75].

Based on these gaps, we empirically assessed the ISCCB in a holistic way by considering factors from PMT, TPB, HBM, SC, personality traits, and work factors such as workload, work emergency, work experience, and IS experience. Additionally, security practices relating to email use, internet use, incident reporting, mobile computing, password management, and information handling [75, 48] were adopted in this work. Healthcare workers

are mostly confronted with, work emergency and workload in their daily duties in healthcare and this can have significant effect in cyber security practice. To the best of our knowledge, none of these previous studies empirically and comprehensively assessed a broad range of the effect of various factors on cyber security practice in healthcare. The theoretical background and hypothesis of our study has been presented in 14.2.2.

14.2.2 Theoretical background and hypotheses

Information security (IS) risk behaviour is a security practice of insiders that has the propensity to violate and compromise organisational security measures [56]. For a healthcare facility to enjoy the benefits associated with the use of information systems, it needs to work to reduce these behavioural risks by improving upon the staff's ISCCB . Security practices are rules that rules the leaders lay down in healthcare facilities requiring the healthcare staff to abide by these in order to enhance the CIA of the healthcare systems and assets. The compliance can be influenced by the knowledge, attitude, and behaviour (KAB) of the healthcare staff, among other factors. Adapting from PMT, TPB, HBM, SC, personality traits, and work factors, we investigated broad range of constructs as shown in Table 14.1.

These factors were related to the security practice measures as shown in Figure 14.1, having associated the measures with both the IS risk of perception as independent variables and the risk of KAB as dependant variables.

This approach is more comprehensive and covers healthcare staff behavioural factors that commonly have an effect on IS security [74, 73, 75] in healthcare. Though other factors such as organisational factors, and leadership play a significant role in IS , our scope and focus are on factors that relate to the healthcare staff in this work.

14.2.2.1 Theory of planned behaviour and knowledge, attitude and behaviour

Ajzen et al. proposed theory of planned behaviour (TPB) that explains the effect of attitude, subjective norms, and behavioural control on the behaviour of individuals [3, 56]. As "As Safa et al. and Parsons et al. explained, attitude relates to a person's beliefs and feelings which are directly influenced by what they know (K) of the IS measures. Both attitude and knowledge can have a direct and indirect effect on the individual's security practice. Therefore the ISCCB is a function of the knowledge and attitude towards the security policies that healthcare management keeps in place. Information security conscious care behaviour is actually the level of compliance with the IS policies that healthcare management keeps in place. The KAB of the healthcare staff tend to be risky if the compliance level tends to compromise CIA of healthcare systems and assets. Healthcare staff's knowledge

Table 14.1: Study constructs and their theoretical origin

No.	Construct	Theory
1	Perceived vulnerability risk	PMT
2	Cues to action with risk	HBM
3	Response efficacy risk	PBM, PMT
4	Self efficacy risk	PMT, HBM
5	Punishment severity risk, Social bonding risk	Social control
6	IS culture risk	TPB
7	Perceived barriers risk	HBM, PMT
8	Agreeableness, Conscientiousness, Extraversion, Openness, Neurotism	Personality
9	Workload, work emergency	
10	Information security knowledge (ISK) risk	
11	Information security attitude (ISA) risk	
12	Information security self-reported conscious care behaviour (ISCCB) risk	

of the security policies also has a direct effect on their attitude. The knowledge is often acquired through their experience, observations, training, and awareness [2]. The staff's attitude towards IS policies refers to their positive or negative intentions towards a specific behaviour. It is a learned tendency to behave in a particular way towards a security policy [41]. As the knowledge of a particular policy influences attitude, the relative behaviour in that context is adjusted accordingly. Attitude has explicit and implicit dimensions. In the explicit attitude, the individuals are aware of the effect of their behaviour while in the implicit attitude, the individuals are not conscious of the effect of their behaviour [6]. Various studies showed significant correlations between these constructs in the context of IS behaviour [65, 48].

In this study, we hypothesize that

- H1: Low level of staff's ISK risks have a positive correlation with ISCCB risk.
- H2: Low level of staff's ISA risks have a positive correlation with ISCCB risk.

Furthermore, the healthcare environment is associated with work emergencies, such as accident cases and other life-threatening health conditions

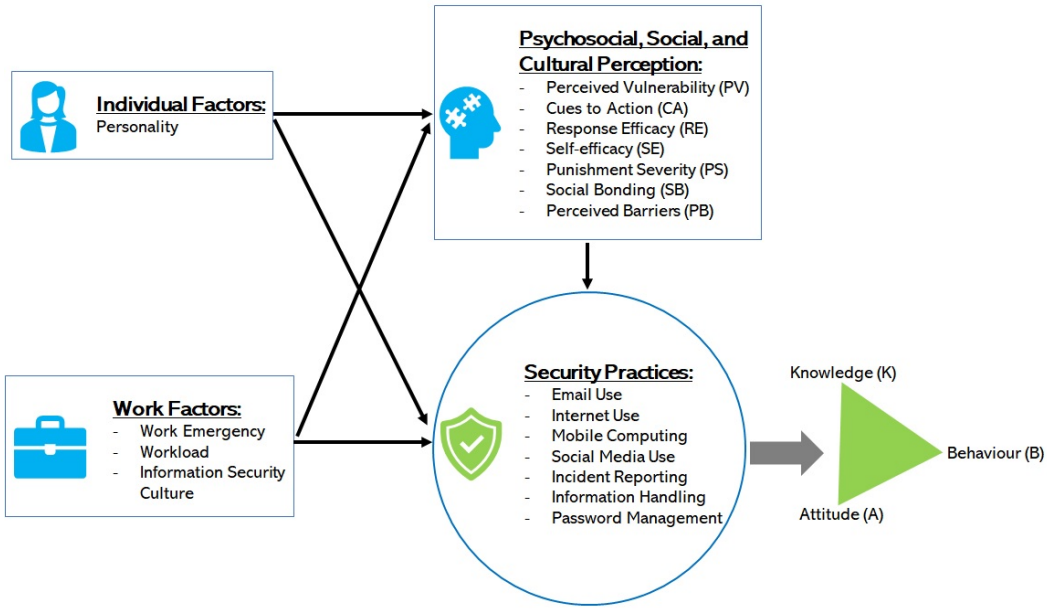


Figure 14.1: The study model

[75, 19, 36]. These cases mostly require urgent and timely interventions from the healthcare professionals without which the patient's condition could worsen. Therefore it is important that hospitals have dedicated units or departments for emergency cases equipped with resources to provide timely interventions for emergency patients. Additionally, a high workload on healthcare personnel has become a huge burden on the few staff which is threatening the effectiveness of health delivery [9]. This has various reasons, including funding gaps and an increase in the patients-to-clinicians ratio [46, 74]. The spontaneous question is, how do healthcare workers observe good security practice amidst work emergencies and high workloads? To this end, we hypothesize that

- H3a: work emergency (WE) is a positive predictor of high risk in the hospital staff's self-reported ISCCB.

- H3b: WE is a positive predictor of high risk in the hospital staff's self-reported ISK.

- H3c: WE is a positive predictor of high risk in the hospital staff's self-reported ISA.
- H3d: work load (WL) is a positive predictor of high risk in the hospital staff's self-reported ISCCB.
- H3e: work load (WL) is a positive predictor of high risk in the hospital staff's self-reported ISA.
- H3f: work load (WL) is a positive predictor of high risk in the hospital staff's self-reported ISK.
- H3g: High risk of IS culture (ISC) is a positive predictor of high risk in the hospital staff's self-reported ISCCB.
- H3h: High risk of IS culture (ISC) is a positive predictor of high risk in the hospital staff's self-reported ISK.
- H3i: High risk of IS culture (ISC) is a positive predictor of high risk in the hospital staff's self-reported ISA.

14.2.2.2 Personality, Knowledge, Attitude and Behaviour (KAB)

Personality traits are inherent characteristics of individuals which are developed from biological and environmental factors [27, 1]. It is a psychological attribute that have an influence on security practice [43]. Others have the view that personality traits are more stable over time when compared with attitude construct [75, 67, 43, 61]. Essentially, there are five common personality traits as outlined and defined below [67, 43, 61]:

- Agreeableness is a measure of an individual's tendencies with respect to social harmony. This trait reflects how well the individual gets along with others, how cooperative or sceptical they are, and how they might interact within a team.
- Conscientiousness is a measure of how careful, deliberate, self-disciplined, and organised an individual is. Conscientiousness is often predictive of employee productivity, particularly in lower-level positions.
- Extraversion is a measure of how sociable, outgoing, and energetic an individual is. Individuals who score lower on the extraversion scale are considered to be more introverted, or more deliberate, quiet, low-key, and independent. Some types of positions are better suited for individuals who fall on one side of the spectrum or the other.
- Openness measures the extent to which an individual is imaginative and creative, as opposed to down-to-earth and conventional.

- Neuroticism or stress tolerance measures the ways in which individuals react to stress.

In measuring the security practice of healthcare staff, we hypothesize that:

- H4a: Healthcare staff personality traits of agreeableness has negative significant correlation with information security knowledge risk.
- H4b: Healthcare staff personality traits of agreeableness has a negative significant correlation with information security attitude risk.
- H4c: Healthcare staff personality traits of agreeableness has a negative significant correlation with ISCCB risk.
- H4d: Healthcare staff personality traits of conscientiousness has a negative significant correlation with information security knowledge risk.
- H4e: Healthcare staff personality traits of conscientiousness has a negative significant correlation with information security attitude risk.
- H4f: Healthcare staff personality traits of conscientiousness has a negative significant correlation with ISCCB risk.
- H4g: Healthcare staff personality traits of openness has a negative significant correlation with information security knowledge risk.
- H4h: Healthcare staff personality traits of openness has a negative significant correlation with information security attitude risk.
- H4i: Healthcare staff personality traits of openness has a negative significant correlation with ISCCB risk.
- H4j: Healthcare staff personality traits of neuroticism has a positive significant correlation with information security knowledge risk.
- H4k: Healthcare staff personality traits of neuroticism has a positive significant correlation with information security attitude risk.
- H4l: Healthcare staff personality traits of neuroticism has a positive significant correlation with ISCCB risk.
- H4j: Healthcare staff personality traits of extroversion has a negative significant correlation with information security knowledge risk.
- H4k: Healthcare staff personality traits of extroversion has a negative significant correlation with information security attitude risk.
- H4l: Healthcare staff personality traits of extroversion has a negative significant correlation with ISCCB risk.

14.2.2.3 Perception

Psychological, social, and cultural perception in relation to information security effects has largely been considered very important in assessing human factors in IS [56, 33, 7]. Therefore, we included perceived vulnerability risk (PV), perceived cues to action risk (CA), response efficacy risk (RE), perceived self-efficacy (SE), punishment severity risk (PS), SC, or informal social control risk (SB) and perceived barrier risk (PB). These were drawn from HBM [52], PMT [54, 7] and SC [15]. These variables were in line with the study objectives and were formed from various psychological, social, and cultural theories. In this regard, we hypothesised that:

- H5a: High WE is a predictor of high risk of PV
- H5b: High WE is a predictor of high risk of CA
- H5c: High WE is a predictor of high risk of RE
- H5e: High WE is a predictor of high risk of SE
- H5f: High WE is a predictor of high risk of PS
- H5g: High WE is a predictor of high risk of SB
- H5h: High WE is a predictor of high risk of PB
- H5a: High WL is a predictor of high risk of PV
- H5b: High WL is a predictor of high risk of CA
- H5c: High WL is a predictor of high risk of RE
- H5e: High WL is a predictor of high risk of SE
- H5f: High WL is a predictor of high risk of PS
- H5g: High WL is a predictor of high risk of SB
- H5h: High WL is a predictor of high risk of PB
- H5i: Poor IS culture is a predictor of high risk of PV
- H5j: Poor IS culture is a predictor of high risk of CA
- H5k: Poor IS culture is a predictor of high risk of RE
- H5l: Poor IS culture is a predictor of high risk of SE
- H5m: Poor IS culture is a predictor of high risk of PS
- H5n: Poor IS culture is a predictor of high risk of SB

- H5o: Poor IS culture is a predictor of high risk of PB
- H5Hi:poor IS culture is a predictor of high risk of PB

With regards to personality traits and perception, we opined that

- H5: Extroversion is a predictor of the risk of CA (H5a), RE (H5b), SE (H5c), PS (H5e), SB (H5f), ISC (H5g), and PB (H5h)
- H6: Agreeableness is a predictor of the risk of CA (H6a), RE (H6b), SE (H6c), PS (H6e), SB (H6f), ISC (H6g), and PB (H6h)
- H7: Conscientiousness is a predictor of the risk of CA (H7a), RE (H7b), SE (H7c), PS (H7e), SB (H7f), ISC (H7g), and PB (H7h)
- H8: Openness is a predictor of the risk of CA (H8a), RE (H8b), SE (H8c), PS (H8e), SB (H8f), ISC (H8g), and PB (H8h)
- H9: Neuroticism is a predictor of the risk of CA (H9a), RE (H9b), SE (H9c), PS (H9e), SB (H9f), ISC (H9g), and PB (H9h)

14.3 Our Approach

14.3.1 Participants, study approval and consent, and data collection

Convenience sampling was adopted in the recruitment process of the hospitals and their participants. First, healthcare facilities that adopted "folderless" systems were invited to join the survey. Some health facilities in Ghana volunteered to take part in the study. Based on ethical, privacy, and security reasons, the names and locations of these facilities have not been mentioned in this paper but ethical clearance was duly obtained in Ghana. Following that, research coordinators were appointed and liaised with thethe hospitals' management teams (i.e. the administrators and medical directors). The healthcare staff who already formed social network groups, were invited to to participate in the online survey. The online questionnaire link was therefore shared on the network, and participants who consented to the study, subsequently responded to the questionnaire . Due to the high cost of the internet data bundles in Ghana, the participants were to fill out the questionnaire and receive a reimbursement of their internet data of an estimated amount of GHS 10.00 (which is about 1.67 United States dollars). There was a consent form to which each participant agreed prior to taking part in the survey. The survey started in March 2021 and was closed in May 2021 of which a total of 233 (female=114, male = 119) delivered their responses however, 212 responses were assessed to be valid responses based on attention checkers that were placed in the questionnaire instrument [10, 16, 35, 38, 48, 25].

14.3.2 Instrument and measurements

This statistical survey was conducted based on earlier studies [72, 74, 75, 73], where a comprehensive security practices were identified [72, 75, 49] and psychological, social, and cultural factors [75, 73] were also identified. The questionnaire instrument was developed with 44 security practice measures to measure the KAB risk in relation to other factors of the healthcare staff [49]. The structure for the questionnaire items is shown in Appendix 14.7. The questionnaire items were developed to measure the psychological, social, and cultural perceptions of the end users in the hospital. Seven questions also covered the staff demographics, and two items each were developed to respectively measure the workload, work emergency, and personality constructs of the healthcare staff. The brief version of personality items was used [25] because the healthcare workers do not have much time to answer the entire 240 items of the long personality scale. In addition, as the main focus of this study is not about personality, the short version has been assessed to meet the scale requirements [25, 22, 7, 49]. The entire instrument for this study was pretested by combining conventional pretesting [20, 57, 42] and a behaviour coding method [53, 11]. The issues with the questionnaire were then identified to include unclear questions, the insignificant differences between questions, problematic questions, inadequate questions, complex terms, and there being too many. A total of 50 questionnaire items were identified to have problems after conducting the pretesting with a total of 36 respondents in behaviour coding and 21 respondents in conventional pretesting. The synergy of the pretesting was necessary to ensure a thorough assessment of the questionnaire for effective correction prior to actual use. Therefore, the identified errors were corrected prior to actually using of the instrument.

Three attention checkers were introduced in the study and required the respondents to select specific answers. Respondents who answered at least two of these checkers wrongly suggest that they did not really pay attention while responding to the instrument. This is one of the common methods used in surveys and it does not affect the validity of the instrument [10, 16, 35, 38, 48, 25].

14.3.3 Statistical analyses

Pearson's correlation, correlation, descriptive statistics, and statistical hypothesis testing methods were used in the analysis and tests. The choice was based on the specific characteristics of the data set involved. For instance, aside from the IS risk behaviour, ISK risk and ISA risk were slightly skewed as shown in Figure 14.5 and Table 14.5. Therefore, Pearson's correlation was adopted as the distribution was approximately normal [32, 65]. Furthermore, t-test and Kruskal Wallis non-parametric one way ANOVA

Table 14.2: Rule of Thumb on Cronbach's Alpha [59, 30]

Alpha Coefficient Range	Strength of association
<0.6	Poor
0.6 to < 0.7	Moderate
0.7 to <0.8	Good
0.8 to <0.9	Very Good
0.9 to 1	Excellent

methods were adopted based on the nature of the data-set in the test scenario. Levene's tests were performed, when required, to determine the variation significance among the test groups [22].The IBM SPSS statistical package version 7 was used for the data analysis. The reliability of the constructs was measured using Cronbach's alpha. Reliability is the extent to which the items are measuring the same underlying construct [8]. The coefficient of the Cronbach's alpha value is usually ranges between 0 and 1 but it is mostly expected to be above 0.6. However, these values are dependent on the number of items in the scale [59, 30, 47, 14, 70]. If the number of items in a scale is 10 or more, it is reasonable to record the coefficient of Cronbach's alpha to be 0.6 or higher (as shown in Table 14.2) [59, 30] otherwise, it is normal to record the Cronbach's alpha values to be as lower with an optimal range of 0.2 to 0.4 [10, 16, 35, 38, 48, 25].

14.4 Results

This section presents the findings of the analysis. As shown in Table 14.3, the reliability statistics of the Cronbach's alpha of all the constructs were within the range of moderate and good strength. Those scales in which the number of items were less than 10 also fell within the optimal range of 0.2 to 0.4 alpha coefficient. To this end, the results of the various factors are presented in the subsequent subsections.

The normality of the distribution of the responses was also checked to guide in choosing methods for the analysis. Absolute skewness of less than 0.5, suggests that the distribution is pretty symmetric but if the skewness is between 0.5 and 1, then it is slightly skewed [28]. Skewness that is greater than 1 or less than - 1 means that it is highly skewed. Additionally, a perfect normal distribution has a kurtosis of zero. Considering means of the distributions in Figure 14.5 (1.59) of ISK risk and in Figure 14.5 (1.88) of ISA risk of the responses, more healthcare workers tend to have less risky ISA practice and ISA risk; however, the security practice pattern in the ISCCB risk showed fairly uniform distribution, suggesting that distribution of healthcare workers in terms of their risk behaviour is uniform in both high-risk

Table 14.3: Reliability statistics

Constructs	Cronbach's Alpha	Cronbach's Alpha based on standardized items	N of items
Psycho-socio-cultural Cyber Security Practice	0.739	0.729	44
Information Security Risk Knowledge (ISK)	0.551	0.566	9
Information Security Risk Attitude (ISA)	0.652	0.654	13
Information Security Risk Conscious Care Behaviour (ISCCB)	0.622	0.612	10
Perceived Barriers (PB)	0.769	0.776	3
Perceived Vulnerability (PV)	0.021	0.018	3
Cues to Action (CA)	0.505	0.543	5
Response Efficacy (RE)	0.481	0.472	3
Perceived Self-fficacy (SE)	0.413	0.406	3
Punishment Certainty (PC)	0.600	0.585	6
Social Bonds and Pressure (SB)	0.633	0.645	7
Cultural factors (CF)	0.462	0.518	5

and low-risk regions.

14.4.1 Nature of the respondents

With reference to Figure 14.2 and Table 14.4, the participants of the study included various groups such as administrative officers (including CEO, top-level management, etc.), pharmacists (including dispensing personnel), doctors (all physicians and physician assistants), nursing (all categories of nurses including nurse assistant), IT personnel (including all IT staff), researcher/research assistant, and statisticians. Other groups who also took part in the study were public health officers, claims officer, health information officers, physiotherapists, records officers, clinical laboratory personnel, and internal auditor. These were categorised into operational staff (doctors, nurses, IT staff, equipment engineers, etc.), managers and supervisors and those in the executive category (including CEO, director, top-level management, etc.).

Two hundred and twelve valid participants took part in the analysis, with averagely, the same proportion of representation of males (50.5%) and females (49.5%) as shown in Table 14.4. Out of this, nurses constituted majority of the group (50.9%) followed by clinical laboratory personnel (9.9%)

Table 14.4: Participants' demographics

Variable	Category	N	%
Gender	Male	107	50.5%
	Female	105	49.5%
Age	17-20	2	0.9%
	21-30	77	36.3%
	31-40	104	49.1%
	41-50	20	9.4%
	51-60	8	3.8%
	Over 60	1	0.5%
Position	Administrative Officer (including CEO, top level management, etc.)	12	5.7
	Pharmacists (including dispensing personnel)	14	6.6
	Doctor (All physicians and physician assistants)	18	8.5
	Nursing (All categories of nurses including nurse assistant)	108	50.9
	IT Personnel (Including all IT staff)	12	5.7
	Researcher/Research Assistant	2	0.9
	Statistician	2	0.9
	Public Health Officer	6	2.8
	Claims Officer	3	1.4
	Health Information Officer	5	2.4
	Physiotherapist	3	1.4
	Records Officer	4	1.9
	Clinical Laboratory Personnel	21	9.9
	Internal auditor	2	0.9
	Total	212	100.0
Position Level	Operational staff (Doctors, Nurses, IT staff, equipment engineer, etc.)	165	77.8%
	Managers and supervisors	44	20.8%
	Executive (including CEO, director, top level management, etc.)	3	1.4%
Experience	Less than 1 Year	19	9.0%
	1-5 Years	83	39.2%
	6-10 Years	53	25.0%
	11-15 Years	40	18.9%
	16-20 Years	9	4.2%
	21-25 Years	5 417	2.4%
	Greater than 25	3	1.4%

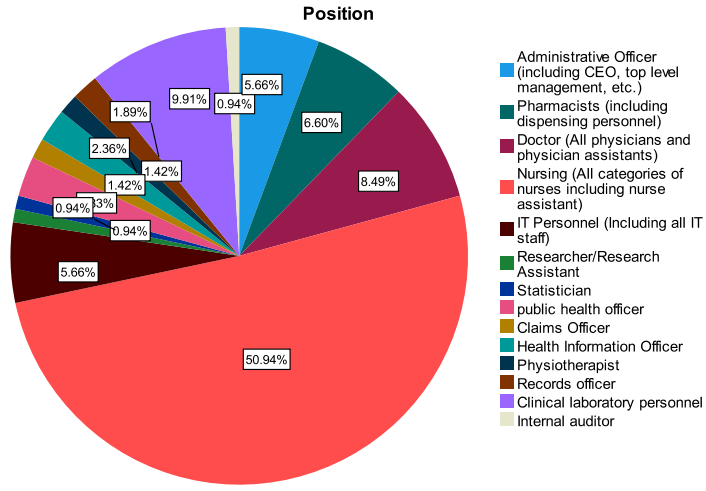


Figure 14.2: Role categories of Respondents

and doctors (8.5%). Additionally,the young age group constituted the majority of between 21 years to 40 years as shown in Figure 14.4. In terms of gender among the hospital roles, female nurses were more prevalent and constituted about 68.7% of the female working population followed by 33.34% of male nurses among the males' healthcare workers as shown in Figure 14.3. Comparatively, few of the workers (8.9%) had less than one year of healthcare experience as a higher proportion of the workers (39.15%) had between 1 to 5 years experience and beyond as shown in Table 14.4.

From the total number of 42 questionnaire items which measured the intended security practice in terms of KAB risks, the ISK risk was averagely lower, followed by ISA risk however, ISCCB risk was comparatively higher as shown in Figure 14.4.

Figure 14.5 and Table 14.5 showed the distribution of responses of the intended security practice in terms of KAB. The number of respondents (frequency) was distributed over the IS security risk intention practices from low (1=Agree) to high risk IS practice (5=Disagree). Knowledge - and attitude - related risks were positively skewed while behaviour risks showed uniform distribution.

14.4.2 Work factors in relation to security risk knowledge, attitude and behaviour (KAB)

In assessing the correlation of work factors (workload and work emergency) as shown in the Table 14.6, ISCCB risk has a a very weak, positive, signifi-

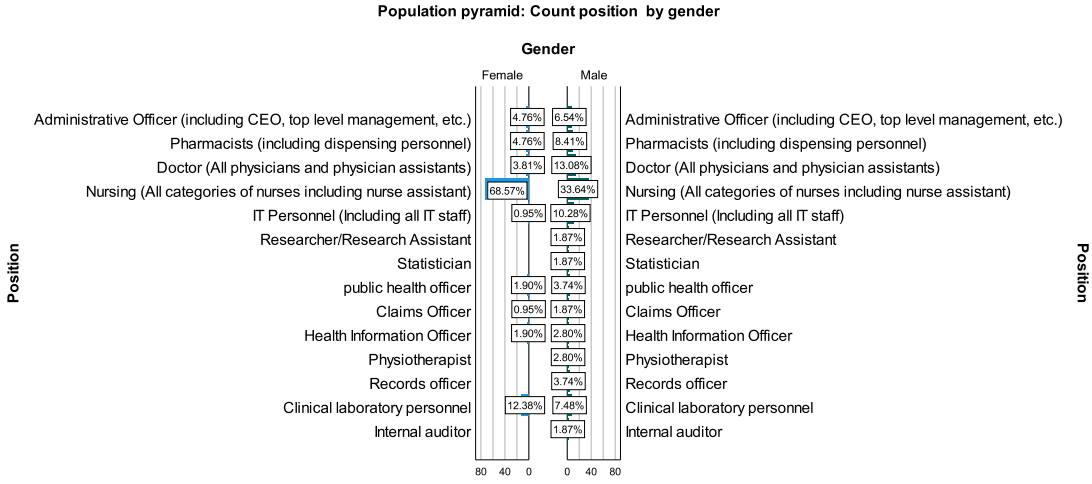


Figure 14.3: Position distribution by gender

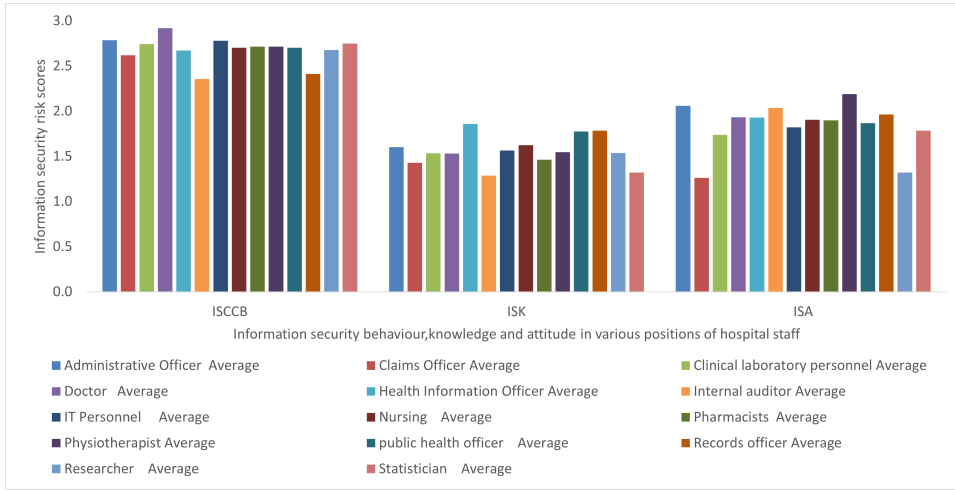


Figure 14.4: Comparison of KAB security practice risk among healthcare staff

cant correlation with work emergency (r=0.195, p=0.01) which in part, supports our hypothesis H3d. ISCCB risk and ISK risk also have a positive weak correlation (r=0.287, p=0.01) as proposed in hypothesis H1. Additionally, ISCCB and ISA risk were moderately and positively correlated (r=0.380,

Table 14.5: Skewness of IS security practice

		IS risk knowledge	IS risk attitude	IS risk behaviour
N	Valid	212	212	212
	Missing	0	0	0
Mean		1.5947	1.8841	2.7244
Std. Deviation		.41645	.49570	.40940
Skewness		.765	.657	.238
Std. Error of Skewness		.167	.167	.167
Kurtosis		.562	.155	-.050
Std. Error of Kurtosis		.333	.333	.333

Table 14.6: Correlations among work load, work emergency, security risk of knowledge, attitude, and behaviour

	Work load	Work Emergency	ISK	ISA	ISCCB
Workload	1	.420**	.011	.005	.011
Work Emergency	.420**	1	-.040	-.042	.195**
ISK	.011	-.040	1	.578**	.287**
ISA	.005	-.042	.578**	1	.380**
ISCCB	.011	.195**	.287**	.380**	1

**. Correlation is significant at the 0.01 level (2-tailed).

p=0.01) as indicated in hypothesis H2. However, the workload was insignificantly correlated (P = 0.005, and r=0.011) with all of the KAB risk variables.

14.4.3 Correlations between personality traits and security risk of KAB

In analysing personality traits and the security risks of KAB, agreeableness has a significant negative and low weak correlation with both ISK risk (-0.166) and ISA risk (-0.140) at a p-value of 0.05 stated in hypotheses H4a and H4b respectively. However it had no significant correlation with IS risk behaviour as shown in the Table 14.7. Therefore, staff who have an agreeable personality, may have low-risk security practices in terms of knowledge and attitude. However, conscientiousness and ISCCB showed a positive and weak significant correlation (0.157) at a p-value of 0.05, suggesting that healthcare workers with conscientiousness traits may tend to be in the high-risk category of IS risk behaviour as suggested in hypothesis H4f.

Table 14.7: Correlations between personality traits, and security practice (KAB)

	ISB	ISK	ISA	E	A	C	N	O
ISB								
ISK	.247**							
ISA	.354**	.567**						
E	0.022	-0.042	-0.043	–				
A	0.124	-.166*	-.140*		–			
C	.157*	-0.049	0.033	0.042	.211**	–		
N	0.132	0.054	0.047	.158*	.360**	0.108	–	
O	-0.11	-0.027	-0.128	.180**	.228**	0.058	.311**	–

**. Correlation is significant at the 0.01 level (2-tailed).
**. Correlation is significant at the 0.05 level (2-tailed).
Extroverted (E), Agreeableness(A), Conscientiousness (C), Neuroticism (N), Openness (O)

14.4.4 Correlations between perception and personality traits

As shown in Table 14.8, healthcare staff with agreeable traits have significant positive and weak correlation (r = 0.163, p-value = 0.05) with SE risk (H6c), but showed negative and weak correlation (r = 0.147, p-value = 0.05) with PS risk (H6e). In addition, Cuest to action risk showed positive correlation with conscientiousness (r = 0.159, p-value = 0.05) as stated in hypothesis (H7a) and Neuroticism (r=0.152, p-valu e= 0.05) (H9a). Meanwhile, openness also has a significant weak and negative correlation with social bonding (r = -0.170, p-value = 0.05)and this supports hypothesis (H8f) .

14.4.5 Perception in relation to work factors

The analysis of the psychological, social, and cultural perceptions in relation to work factors such as workload, hospital security culture, and work emergency are shown in Table 14.9. The perception variables have an insignificant correlation with work emergency and workload. However, RE and PS risks respectively have a significant negative and weak correlation with hospital IS the culture of (r = -0.182, p-value = 0.05) and (r = -0.177, p-value = 0.01) as stated in hypotheses H5K and H5m respectively.

14.4.6 Statistical tests of IS risk knowledge, attitude, and behaviour (KAB) with categorical variables

Statistical tests were conducted to assess the distribution of IS risk KAB across categorical variables, including gender, position levels, hospital IS experience, age group, and healthcare work experience. T-test was used

Table 14.8: Correlations between perception and personality

	CA	RE	SE	PS	SB	IS culture	PB	E	A	C	N	O
CA	–											
RE	.182*	–										
SE	.310**	.335**	–									
PS	.282**	0.065	.221**	–								
SB	.363**	.189*	.202*	.340**	–							
IS culture	.165*	0.041	.167*	.353**	.308**	–						
PB	0.131	.275**	.197*	.285**	.377**	.271**	–					
E	0.123	-0.096	0.069	-0.029	-0.002	0.045	-0.023	–				
A	0.069	0.060	.163*	-.147*	-0.129	-0.070	-0.039	.361**	–			
C	.159*	-0.057	0.122	-0.018	0.115	-0.009	0.044	.166*	.288**	–		
N	.152*	0.063	0.146	0.019	0.027	0.044	0.090	.278**	.342**	.175*	–	
O	-0.092	-0.078	0.027	-0.087	-.170*	-0.130	0.003	.212**	.237**	0.022	.319**	

**. Correlation is significant at the 0.01 level (2-tailed).
**. Correlation is significant at the 0.05 level (2-tailed).
Extroverted (E), Agreeableness(A), Conscientiousness (C), Neuroticism (N), Openness (O)

for the hypothesis between gender and KAB risk variables since it is normally used for testing 2-level categorical variables with continuous variables. Additionally, Levene's test, did not show significant variances among the group's population of the three respective KAB variables(r = 0.412, r = 0.406, r= 0.632) at a p-value of 0.05.

Furthermore, Kruskal Wallis non-parametric one way ANOVA was used in the hypothesis testing with the remaining variables such as position levels, hospital IS experience, age group, and healthcare work experience as they were more than two levels. Aside from work experience in healthcare, the statistical tests show that the distribution of IS risk of KAB is the same across all variables. With regards to experience in healthcare, the distribution of ISK and ISA risks were uniform across all healthcare experience groups, but the distribution of IS risk behaviour across all work experience groups did not show uniform distribution with a significance level of (r = -0.00, p-value = 0.05) as shown in Table 14.10.

Therefore, the post-hoc pairwise test was analysed to determine the distribution among the groups. The results indicate that there are significant difference (p-value = 0.05) of IS security behaviour among various groups such as 7(¿ 25years)-2(1 to 5 years) = (0.019), 7(¿25)-4(11 to 15) = 0.013, 7(¿25)-3(6 to 10) = 0.003,7(¿25)-5(16 to 20years) = 0.001, 7(¿25)-6(21-25years) = 0.002 and others as shown in Table 14.11 at significance level of 0.05 or less.

Table 14.9: Correlations between perception and work factors

	CA	RE	SE	PS	SB	IS culture	PB	WL	WE	Hospital Culture	IS
CA	–										
RE	.182*	–									
	0.016										
	173	173									
SE	.310**	.335**	–								
PS	.282**	0.065	.221**	–							
SB	.363**	.189*	.202*	.340**	–						
IS culture	.165*	0.041	.167*	.353**	.308**	–					
PB	0.131	.275**	.197*	.285**	.377**	.271**	–				
WL	-0.028	-0.044	-0.023	0.040	-0.011	0.001	0.019	–			
WE	0.015	0.026	0.079	-0.028	0.004	0.106	0.127	.430**	–		
Hospital IS Culture	-0.007	-.182*	-0.076	-.177**	-0.034	-0.068	-0.064	0.059	0.127	–	

**. Correlation is significant at the 0.01 level (2-tailed).
**. Correlation is significant at the 0.05 level (2-tailed).

14.5 Discussion

This study assessed various factors that affect sound security and privacy behaviour among healthcare workers. The purpose was to assess gaps in their security practice and to find out if some of the factors had negative effects on the security practices. This would provide guidance for the choice of better mitigation strategies such as incentive measures to improve security practices. This study is centred on the human element which is one of the three pillars of effective cyber security practice processes, technology, and the people [21, 12].

14.5.1 Principal findings

The study was characterised by almost equal proportion of male and female participants and was also dominated with nurses more than half (50.9%) of the total participants. In terms of distribution of the risk of security practice in the aspect of KAB, there was generally uniform distribution of the behaviour risk while ISK and ISA risks slightly skewed to the positive side

Table 14.10: Kruskal Wallis non parametric one way ANOVA with work experience and KAB

	Null Hypothesis	Test	Sig.a,b	Decision
1	The distribution of ISCCB risk is the same across categories of experience in healthcare.	Independent-Samples Kruskal-Wallis Test	0.000	Reject the null hypothesis.
2	The distribution of ISK risk is the same across categories of experience in healthcare.	Independent-Samples Kruskal-Wallis Test	0.624	Retain the null hypothesis.
3	The distribution of ISA risk is the same across categories of experience in healthcare.	Independent-Samples Kruskal-Wallis Test	0.582	Retain the null hypothesis.

as shown in Figure 14.5. The results further showed a significant positive and weak correlation between ISK risk, ISA, work emergency, and ISCCB as shown in Table 14.6 and Table 14.12. Additionally, while agreeableness had a negative and weak correlation with ISK and ISA, conscientiousness had a significant positive and weak correlation with ISCCB as shown in Table 14.9 and Table 14.12. Essentially, Table 14.12 consists of the gist of the study results that showed significant correlations. These are further discussed in the subsequent subsections.

As shown in Table 14.12, aside the results values of hypothesis H1a, and

Table 14.11: Post-hoc pairwise test with null hypothesis:Sample 1 and sample 2 distribution are the same

Sample 1(Year)-Sample 2(Year)	Test Statistic	Std. Error	Std. Test Statistic	Sig.
7(>25)-1(<1)	55.263	38.080	1.451	0.147
7(>25)-2(1 to 5)	84.476	36.022	2.345	0.019
7(>25)-4(11 to 15)	91.550	36.692	2.495	0.013
7(>25)-3(6 to 10)	109.623	36.376	3.014	0.003
7(>25)-5(16 to 20)	130.667	40.863	3.198	0.001
7(>25)-6(21-25)	137.700	44.763	3.076	0.002
1(<1)-2(1 to 5)	-29.213	15.589	-1.874	0.061
1(<1)-4(11 to 15)	-36.287	17.078	-2.125	0.034
1(<1)-3(6 to 10)	-54.359	16.390	-3.317	0.001
1(<1)-5(16 to 20)	-75.404	24.803	-3.040	0.002
1(<1)-6(21-25)	-82.437	30.808	-2.676	0.007
2(1 to 5)-4(11 to 15)	-7.074	11.798	-0.600	0.549
2(1 to 5)-3(6 to 10)	-25.147	10.777	-2.333	0.020
2(1 to 5)-5(16 to 20)	-46.191	21.511	-2.147	0.032
2(1 to 5)-6(21-25)	-53.224	28.225	-1.886	0.059
4(11 to 15)-3(6 to 10)	18.073	12.838	1.408	0.159
4(11 to 15)-5(16 to 20)	-39.117	22.614	-1.730	0.084
4(11 to 15)-6(21-25)	-46.150	29.075	-1.587	0.112
3(6 to 10)-5(16 to 20)	-21.044	22.098	-0.952	0.341
3(6 to 10)-6(21-25)	-28.077	28.676	-0.979	0.328
5(16 to 20)-6(21-25)	-7.033	34.189	-0.206	0.837

H2 that have the correlation strength of moderate, the remaining results falls within the low or weak category of the correlation strength [64]. This suggests that with low strength in correlation, because the findings are statistically significant, the chances or the probability of their predictions are merely low while the findings with the modest strength has a higher prediction probability. This suggests that the findings are still valid as the results are significant and have the probability of prediction.

Table 14.12: Summary of results

No	Variable 1-Variable 2	Value	Hypothesis
1	Work Emergency-ISCCB	.195**	H3d
2	ISA-ISK	.578**	H1a
3	ISA-ISCCB	.380**	H2
4	ISK-ISCCB	.287**	H1
5	ISCCB-Conscientiousness	.157*	H4f
6	ISA-Agreeableness	-0.1407*	H2
7	ISK-Agreeableness	-.166*	H1
8	Self Efficacy-Agreeableness	.163*	H6c
9	Punishment severity-Agreeableness	.163*	H6e
10	Cuest to action-Conscientiousness	.159*	H7a
11	Cuest to action-Neuroticism	.152*	H9a
12	Social bonding-Openness	-0.170*	H8f
13	Response efficacy risk-Hospital IS Culture	-.182*	H5k
14	Formal social control risk-Hospital IS Culture	-.177**	H5m

14.5.2 Risk of knowledge, attitude, and behaviour(KABs)

The healthcare workers are required to observe security practice in a bit to enhance the systems' CIA. The most common practices include password management, incident reporting, email use, social media use, mobile computing, and information handling [48, 50] as shown in figure 14.1. Mostly, these security practices are observed based on the healthcare facility's security policies which are literally the "law" to be followed by the healthcare workers in order to avoid security breaches. With regards to the model, healthcare workers are characterised with their personalities. In addition to that they are associated with work factors which may contribute to their cyber security perception. How all these variables correlates and affect the KAB of healthcare staff is the oject interest of this study. From our assessment, ISCCB risk positively correlated with both ISK risk and ISA risk with the correlation strength being low and moderate, as shown in Table 14.12. Additionally, ISK and ISA have a modest positive significant correlation. This could mean that better ISK and ISA risks could significantly influence better ISCCB which supports our hypotheses (H1a,H1, and H2). Related studies by [48, 50] found a similar pattern.The comparative advantage here is the comprehensive approach in which results from various constructs were obtained [74]. For instance, healthcare is often characterised with work

emergency of which this was included in the study based on our comprehensive approach. Interestingly, the work emergency correlated with the risk of security behaviour and management can therefore use various state-of-the-arts methods to influence the ISCCB of healthcare workers.

Additionally, the findings also showed a significant positive weak correlation between work emergency and ISCCB as stated in hypothesis H3d, but not workload. It is possible that workload does not create urgency and does not interfere with the healthcare security practice as compared to work emergency [66, 77, 24, 4, 37, 63]. In a healthcare emergency situation, the medical staff main goal is to save the patient's life or prevent the patient's condition from worsening. But in some care situations, observing good information security practice might be least prioritised by the healthcare staff [37, 63] and they may tend to circumvent some of the security and privacy measures to perform their core healthcare functions . As healthcare emergency positively correlated with the ISCCB risk it means that during emergency situation, the risk of complying with security measures is high. To this end, incentive measures including usable security measures are required to promote sound security practice. Otherwise, with all the urgency in healthcare, the severity of the impact of security breaches in healthcare would be much higher [44].

Individual differences were also assessed with the KAB variables. The findings showed that agreeableness has a significant negative weak correlation with ISK risk and ISA risk but not ISCCB. However, healthcare workers with high a conscientiousness trait tend to have a significant positive weak correlation with the risk of ISCCB but not ISK and ISA risks as shown in Table 14.12. With a negative correlation, between the risks of ISK and agreeableness as well as ISA and agreeableness, it implies that the risk of cyber security practice of knowledge and attitude tend to reduce with healthcare workers who have higher scores with agreeable personalities and vice versa. This could be the case because healthcare staff with a high score of agreeableness characteristics tend to easily agree with cyber security education and training, enabling them to have low risk in ISK and ISA. This finding is in line with previous studies [60, 31]. Conversely, the healthcare workers with a high risk score of conscientiousness showed higher ISCCB risk which contrasts our hypothesis and previous studies [60, 31]. Our assumption was that a higher score of conscientiousness would have translated into less risk of ISCCB. It is possible that the workers with a high risk score of conscientiousness equally have high self-esteem, giving them false confidence of conscious care security practices [62].

14.5.3 Personality and psycho-socio-cultural security behaviour

Healthcare workers (just like any person) are complex in nature, and this is exhibited in their ISCCB. For instance, healthcare workers are social beings

[13], who work with friends, family members, and other relations which can have an impact on security measures. This expresses the need to consider social factors in an effort to estimate the security behaviour of a hospital [15, 60, 31, 33, 56].

The results showed that only extroversion did not have a significant correlation with any of the psycho-social-cultural traits but agreeableness was a significant positive weak predictor of SE risk and PS risks. This means that healthcare workers with agreeable characters tend to have high-risk behaviour in terms of SE and PS . Related studies found significant correlations among agreeableness versus SE risk [31, 60] but not SE and agreeableness. Agreeable personality traits correspond to being cooperative, helpful, and kind but require similar treatment [31], and such personalities may feel they will not be punished and would be treated with kindness if they violate security and privacy policies regarding SE and PS.

Also, conscientiousness and neuroticism had a significant positive weak correlation with cues to action. This implies that higher risks of cues to action behaviour corresponded to staff with higher scores in neuroticism and conscientiousness traits. The finding of a higher risk of security practice in relation to neuroticism traits is in line with earlier studies [31, 60, 61, 48] of self-reported cyber security behaviour. Staff with neuroticism traits tend to have higher risk behaviour, suggesting that, emotional stability is a predictor of low cues to action security risk behaviour. Furthermore, self-reported hospital information culture was found to have a significant negative correlation with both response efficacy and punishment severity risks behaviour as shown in Table 14.12 and Table 14.8.This can be interpreted as finding that higher scores or better hospital security culture predicts low risk of both RE and PS risks. This finding is similar to a related study in which subjective norms were found significant to self-reported ISCCB [56]. In this vein, healthcare facility management can improve upon the cyber security practice in the area of response efficacy and punishment severity by improving upon the security culture of the hospital through self-efficacy and punishment severity related incentives.

14.5.4 Implication of the study

The results may not be easily generalised due to the differences in the cyber security culture of each country that affects the healthcare domain, but there are various implications. Firstly, the security knowledge of healthcare staff can be improved to enhance their attitude and behaviour based on the findings and unique characteristics of the healthcare environment. Secondly, usable security measures can be assessed and implemented such, that amidst work emergency, the healthcare staff can subconsciously comply with security and privacy measures. Finally, psychological perceptions in relation to individual factors, such as personality, can be influenced with the state-of-

the-arts training, education and learning (TEL) to improve on security practice. For instance, state-of-the-arts approaches such as virtual reality (VR) is able to elicit 27% higher emotional engagement than television. Also, learners who use VR retain 75% of what they are taught as compared to 10% of that of the traditional methods. Additionally, surgeons trained using VR make fewer errors and spent less time in cases as compared to surgeons who are conventionally trained [29, 39]. Such TEL approaches could induce sound security practices in healthcare.

14.6 Conclusion

Digitising hospital operations into paperless systems has a lot of benefits for management, staff, and patients. However this also comes with its associated risks including the threats of cyber security. Therefore, the security behaviour of healthcare staff was assessed to determine gaps and variables that can be improved towards enhancing conscious care security practice. This study covered individual factors, work factors and psychological social and cultural factors. These were then related with security practices to assess the cyber security knowledge, attitude and behaviour of healthcare staff in an actual healthcare facility.

A survey was conducted in a typical, paperless hospital in Ghana by collecting self-reported cyber-security practices of healthcare staff in psychological, social, and cultural aspects in addition to work-related factors, such as workload and work emergency.

The findings showed that work emergency, ISK risks, and ISA risks have significant positive weak correlation with self-reported ISCCB risks. In the aspect of psycho-socio-cultural behaviour, the study showed that healthcare staff with the higher scores in agreeableness, openness and hospital information security culture tend to respectively have low cyber security risk behaviour in ISK and ISA, social bonding and response efficacy as well as punishment severity. However, consciousness correlated with high risks of information security-conscious care behaviour and punishment severity which is in contradiction with other studies. This implies that usable security measures can be assessed and implemented such that amidst work emergency, the healthcare staff can subconsciously comply with security and privacy measures. Additionally, the security knowledge of healthcare staff can be improved to enhance their attitude and behaviour based on the findings.

This study is limited by the fact that, the study participants were assessed of their intended security practices. Since intended security practice is not the same as actual security practice, future studies should practically examine the effect of psychological incentives on security practices. Also, in this study, the reasons of the correlations are speculative, with the

lack of causality. These are inherent attributes of quantitative survey with correlation analysis. Therefore, future studies should explore a qualitative approach to obtain the nuance of the reasons of the security gaps towards improved decision making for better security countermeasures.

14.7 Appendix 1

- K) I know that visiting any external website with the hospital computing devices at work CAN be harmful to the security of the hospital *
- A) In my opinion, I am confident in myself that I CANNOT be a victim to a malicious attack at work if I visit other websites other than the hospital's website *
- B) I sometimes VISIT at least one of the following websites using the hospital's computer: social media; Dropbox and other public file storage systems; On-line musics or Videos sites; On-line newspapers and magazines; Personal e-mail accounts; Games; Instant messaging services etc *
- K) I know that I have to read alert messages/emails concerning security *
- A) In my opinion, it is IMPORTANT to read the alert messages/emails concerning security *
- B) I do NOT often read the alert messages/emails concerning security *
- K) I know that it is not a good security practice to click on a link in an email from an unknown sender *
- A) Nothing bad can happen if I click on a link in an email from an unknown sender *
- B) I sometimes click on a links in an email from an unknown sender *

14.8 Bibliography

[1] OMSORGSDEPARTEMENTET . How does personality influence your cyber risk?, 2021. https://www.cybsafe.com/community/blog/how-does-personality-influence-your-cyber-risk/. 10, 410

[2] ABAWAJY, J. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology 33*, 3 (2014), 237–248. 10, 408

[3] AJZEN, I., AND MADDEN, T. J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology 22*, 5 (1986), 453–474. 9, 12, 407

[4] ALAMI, H., GAGNON, M.-P., AHMED, M. A. A., AND FORTIN, J.-P. Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. *Health Policy and Technology 8*, 4 (2019), 319–321. 427

[5] ALBARRAK, A. I. Evaluation of users information security practices at king saud university hospitals. *Global Business & Management Research 3*, 1 (2011). 406

[6] ALBRECHTSEN, E. A qualitative study of users' view on information security. *Computers & security 26*, 4 (2007), 276–289. 10, 408

[7] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., AND XU, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. 272, 274, 296, 313, 404, 406, 412, 414, 442, 444, 457, 512

[8] ARACHCHILAGE, N. A. G., AND LOVE, S. A game design framework for avoiding phishing attacks. *Computers in Human Behavior 29*, 3 (2013), 706–714. 415, 501

[9] ASAMANI, J. A., AMERTIL, N. P., AND CHEBERE, M. The influence of workload levels on performance in a rural hospital. *British Journal of Healthcare Management 21*, 12 (2015), 577–586. 409

[10] BERINSKY, A. J., MARGOLIS, M. F., AND SANCES, M. W. Separating the shirkers from the workers? making sure respondents pay attention on self-administered surveys. *American Journal of Political Science 58*, 3 (2014), 739–753. 413, 414, 415, 499, 501, 502

[11] BIEMER, P. Modeling measurement error to identify flawed questions. *Methods for testing and evaluating survey questionnaires* (2004), 225–246. 414

[12] BOWEN, B. M., DEVARAJAN, R., AND STOLFO, S. Measuring the human factor of cyber security. In *2011 IEEE International Conference on Technologies for Homeland Security (HST)* (2011), IEEE, pp. 230–235. 423

[13] BOX, D., AND POTTAS, D. Improving information security behaviour in the healthcare context. *Procedia Technology 9* (2013), 1093–1103. 428

[14] BRIGGS, S. R., AND CHEEK, J. M. The role of factor analysis in the development and evaluation of personality scales. *Journal of personality 54*, 1 (1986), 106–148. 415, 501

[15] CHENG, L., LI, Y., LI, W., HOLM, E., AND ZHAI, Q. Understanding the violation of is security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security 39* (2013), 447–459. 10, 412, 428

[16] CURRAN, P., AND HAUSER, D. Understanding responses to check items: A verbal protocol analysis. In *Philadelphia, PA: Paper presented at the 30th Annual Conference of the Society for Industrial and Organizational Psychology* (2015). 413, 414, 415, 499

[17] DAGLIATI, A., MALOVINI, A., TIBOLLO, V., AND BELLAZZI, R. Health informatics and ehr to support clinical research in the covid-19 pandemic: an overview. *Briefings in bioinformatics 22*, 2 (2021), 812–822. 404

[18] D'ARCY, J., AND LOWRY, P. B. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal 29*, 1 (2019), 43–69. 405

[19] DEVITA, T., BRETT-MAJOR, D., AND KATZ, R. How are healthcare provider systems preparing for health emergency situations? *World Medical & Health Policy* (2021). 409

[20] DRENNAN, J. Cognitive interviewing: verbal data in the design and pretesting of questionnaires. *Journal of advanced nursing 42*, 1 (2003), 57–63. 414

[21] FAIRBURN, N., SHELTON, A., ACKROYD, F., AND SELFE, R. Beyond murphy's law: Applying wider human factors behavioural science approaches in cyber-security resilience. In *International Conference on Human-Computer Interaction* (2021), Springer, pp. 123–138. 423

[22] FERNANDEZ-ALEMAN, J. L., SANCHEZ-HENAREJOS, A., TOVAL, A., SANCHEZ-GARCIA, A. B., HERNANDEZ-HERNANDEZ, I., AND FERNANDEZ-LUQUE, L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics 84*, 6 (2015), 454–467. 12, 15, 200, 406, 414, 415

[23] FURNELL, S., AND CLARKE, N. Power to the people? the evolving recognition of human aspects of security. *computers & security 31*, 8 (2012), 983–988. 404

[24] GHAZVINI, A., AND SHUKUR, Z. Review of information security guidelines for awareness training program in healthcare industry. In

2017 6th International Conference on Electrical Engineering and Informatics (ICEEI) (2017), IEEE, pp. 1–6. 427

[25] GOSLING, S. D., RENTFROW, P. J., AND SWANN JR, W. B. A very brief measure of the big-five personality domains. *Journal of Research in personality 37*, 6 (2003), 504–528. 413, 414, 415, 444, 499, 501, 502

[26] GRASSEGGER, T., AND NEDBAL, D. The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science 181* (2021), 59–66. 405

[27] GRATIAN, M., BANDI, S., CUKIER, M., DYKSTRA, J., AND GINTHER, A. Correlating human traits and cyber security behavior intentions. *computers & security 73* (2018), 345–358. 10, 410

[28] GROENEVELD, R. A., AND MEEDEN, G. Measuring skewness and kurtosis. *Journal of the Royal Statistical Society: Series D (The Statistician) 33*, 4 (1984), 391–399. 415

[29] GURUSAMY, K., AGGARWAL, R., PALANIVELU, L., AND DAVIDSON, B. Systematic review of randomized controlled trials on the effectiveness of virtual reality training for laparoscopic surgery. *Journal of British Surgery 95*, 9 (2008), 1088–1097. 429

[30] HAIR, J. F., PAGE, M., AND BRUNSVELD, N. *Essentials of business research methods*. Routledge, 2019. xx, 294, 415, 501, 502

[31] HALEVI, T., MEMON, N., LEWIS, J., KUMARAGURU, P., ARORA, S., DAGAR, N., ALOUL, F., AND CHEN, J. Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* (2016), pp. 318–324. 427, 428

[32] HAUKE, J., AND KOSSOWSKI, T. Comparison of values of pearson's and spearman's correlation coefficient on the same sets of data. 414

[33] HERATH, T., AND RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems 47*, 2 (2009), 154–165. 7, 405, 412, 428, 448, 457, 493

[34] HOSSAIN, A., QUARESMA, R., AND RAHMAN, H. Investigating factors influencing the physicians' adoption of electronic health record (ehr) in healthcare system of bangladesh: An empirical study. *International Journal of Information Management 44* (2019), 76–87. 404

[35] HUANG, J. L., BOWLING, N. A., LIU, M., AND LI, Y. Detecting insufficient effort responding with an infrequency scale: Evaluating validity and participant reactions. *Journal of Business and Psychology 30*, 2 (2015), 299–311. 413, 414, 415, 499, 501, 502

[36] KHALID, M., AWAIS, M., SINGH, N., KHAN, S., RAZA, M., MALIK, Q. B., AND IMRAN, M. Autonomous transportation in emergency healthcare services: Framework, challenges, and future work. *IEEE Internet of Things Magazine 4*, 1 (2021), 28–33. 409

[37] KOPPEL, R., SMITH, S., BLYTHE, J., AND KOTHARI, V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise*. IOS Press, 2015, pp. 215–220. 427, 468

[38] KUNG, F. Y., KWOK, N., AND BROWN, D. J. Are attention check questions a threat to scale validity? *Applied Psychology 67*, 2 (2018), 264–283. 413, 414, 415, 499, 501

[39] LARSEN, C. R., OESTERGAARD, J., OTTESEN, B. S., AND SOERENSEN, J. L. The efficacy of virtual reality simulation training in laparoscopy: a systematic review of randomized trials. *Acta obstetricia et gynecologica Scandinavica 91*, 9 (2012), 1015–1028. 429

[40] LEBEK, B., UFFEN, J., BREITNER, M. H., NEUMANN, M., AND HOHLER, B. Employees' information security awareness and behavior: A literature review. In *2013 46th Hawaii International Conference on System Sciences* (2013), IEEE, pp. 2978–2987. 406

[41] LEONARD, L. N., CRONAN, T. P., AND KREIE, J. What influences it ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management 42*, 1 (2004), 143–158. 9, 408

[42] MARTIN, E., SCHECHTER, S., AND TUCKER, C. Interagency collaboration among the cognitive laboratories: past efforts and future opportunities. Statistical Policy Working Paper 28: 1998 Seminar on Interagency 414

[43] MCCORMAC, A., ZWAANS, T., PARSONS, K., CALIC, D., BUTAVICIUS, M., AND PATTINSON, M. Individual differences and information security awareness. *Computers in Human Behavior 69* (2017), 151–156. 10, 410

[44] MIDDAUGH, D. J. Cybersecurity attacks during a pandemic: It is not just it's job! *Medsurg Nursing 30*, 1 (2021), 65–66. 427

[45] MIRIOVSKY, B. J., SHULMAN, L. N., AND ABERNETHY, A. P. Importance of health information technology, electronic health records, and continuously aggregating data to comparative effectiveness research and learning health care. *Journal of Clinical Oncology 30*, 34 (2012), 4243–4248. 404

[46] NYAMTEMA, A. S. Bridging the gaps in the health management information system in the context of a changing health sector. *BMC medical informatics and decision making 10*, 1 (2010), 1–6. 409

[47] PALLANT, J. Spss survaival manual: a step by step guide to data analysis using spss, 2010. 415, 501

[48] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., AND ZWAANS, T. The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security 66* (2017), 40–51. 10, 278, 404, 405, 406, 408, 413, 414, 415, 426, 428, 443, 446, 499, 501, 502

[49] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. The development of the human aspects of information security questionnaire (hais-q). 7, 10, 278, 282, 414, 442, 443, 446, 461, 498

[50] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. Determining employee awareness using the human aspects of information security questionnaire (hais-q). *Computers & security 42* (2014), 165–176. 426

[51] POSEY, C., ROBERTS, T. L., AND LOWRY, P. B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems 32*, 4 (2015), 179–214. 405

[52] PRENTICE-DUNN, S., AND ROGERS, R. W. Protection motivation theory and preventive health: Beyond the health belief model. *Health education research 1*, 3 (1986), 153–161. 412

[53] REEVE, B. B., AND MÂSSE, L. C. Item response theory modeling for questionnaire evaluation. *Methods for testing and evaluating survey questionnaires* (2004), 247–273. 414

[54] ROSENSTOCK, I. M. The health belief model and preventive health behavior. *Health education monographs 2*, 4 (1974), 354–386. 412, 443

[55] SAFA, N. S., MAPLE, C., WATSON, T., AND VON SOLMS, R. Motivation and opportunity based model to reduce information security

insider threats in organisations. *Journal of information security and applications 40* (2018), 247–257. 405

[56] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 9, 10, 12, 15, 200, 274, 405, 407, 412, 428, 446, 457

[57] SCHECHTER, S., BEATTY, P., AND BLOCK, A. Cognitive issues and methodological implications in the development and testing of a traffic safety questionnaire. In *Proceedings of the Survey Research Methods Section of the American Statistical Association* (1994), pp. 1215–1219. 414

[58] SCHUMAKER, R. P., AND REGANTI, K. P. Implementation of electronic health record (ehr) system in the healthcare industry. *International Journal of Privacy and Health Information Management (IJPHIM) 2*, 2 (2014), 57–71. 404

[59] SHAH, M. Perception of managers on the effectiveness of the internal audit functions: A case study in tnb. xx, 294, 415, 501, 502

[60] SHAPPIE, A. T., DAWSON, C. A., AND DEBB, S. M. Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media 9*, 4 (2020), 475. 427, 428

[61] SHROPSHIRE, J., WARKENTIN, M., AND SHARMA, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *computers & security 49* (2015), 177–191. 10, 410, 428

[62] SKOREK, M., SONG, A. V., AND DUNHAM, Y. Self-esteem as a mediator between personality traits and body esteem: path analyses across gender and race/ethnicity. *PloS one 9*, 11 (2014), e112086. 427

[63] STOBERT, E., BARRERA, D., HOMIER, V., AND KOLLEK, D. Understanding cybersecurity practices in emergency departments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–8. 427

[64] TAYLOR, R. Interpretation of the correlation coefficient: a basic review. *Journal of diagnostic medical sonography 6*, 1 (1990), 35–39. 425

[65] THIRUMALAI, C., CHANDHINI, S. A., AND VAISHNAVI, M. Analysing the concrete compressive strength using pearson and spearman. In *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)* (2017), vol. 2, IEEE, pp. 215–218. 10, 408, 414

[66] TORRES, H. G., AND GUPTA, S. The misunderstood link: information security training strategy. 427

[67] UFFEN, J., GUHR, N., AND BREITNER, M. H. Personality traits and information security management: An empirical study of information security executives. 10, 410, 442

[68] VAN NIEKERK, J., AND VON SOLMS, R. Information security culture: A management perspective. *Computers & security 29*, 4 (2010), 476–486. 404

[69] VANCE, A., SIPONEN, M., AND PAHNILA, S. Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management 49*, 3-4 (2012), 190–198. 405

[70] VASKE, J. J., BEAMAN, J., AND SPONARSKI, C. C. Rethinking internal consistency in cronbach's alpha. *Leisure Sciences 39*, 2 (2017), 163–173. 415, 501

[71] WILEY, A., MCCORMAC, A., AND CALIC, D. More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security 88* (2020), 101640. 404

[72] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[73] YENG, P. K., SZEKERES, A., YANG, B., AND SNEKKENES, E. A. Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: Systematic mapping study. *JMIR human factors 8*, 2 (2021), e17604. 9, 11, 15, 17, 24, 272, 273, 274, 282, 405, 406, 407, 414, 457, 496, 498

[74] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 11, 15, 22, 138, 200, 217, 224, 236, 273, 274, 404, 406, 407, 409, 414, 426, 442, 491, 498

[75] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 1, 2, 6, 10, 11, 15, 17, 23, 199, 217, 224, 274, 282, 404, 405, 406, 407, 409, 410, 414, 442, 443, 454, 457, 491, 498

[76] YENG P, FAUZI MA, S. L., AND B, Y. Legal aspects of information security requirements for healthcare in three countries: A scoping review as a benchmark towards assessing healthcare security

practices. *JMIR Hum Factors* (2022). Available from: https://humanfactors.jmir.org/2022/0/e0/. 7, 15, 246, 405

[77] ZAFAR, H. Cybersecurity: Role of behavioral training in healthcare. 427

[78] ZANDIEH, S. O., YOON-FLANNERY, K., KUPERMAN, G. J., LANGSAM, D. J., HYMAN, D., AND KAUSHAL, R. Challenges to ehr implementation in electronic-versus paper-based office practices. *Journal of general internal medicine 23*, 6 (2008), 755–761. 404

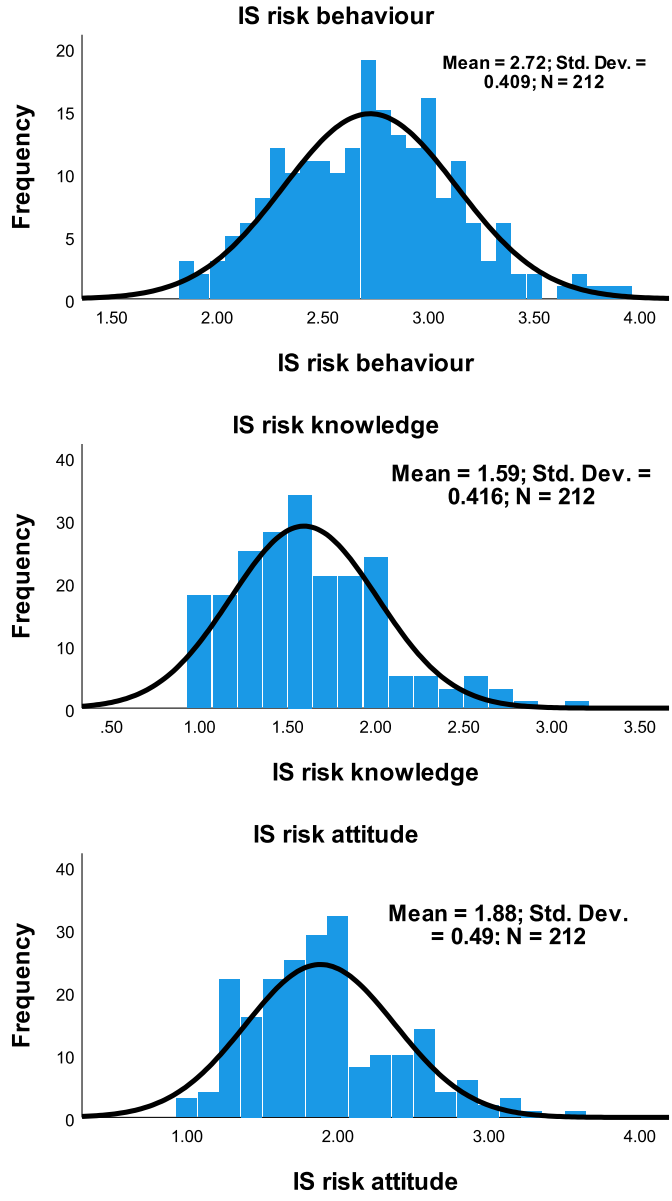


Figure 14.5: Distribution of knowledge, attitude and behaviour of security practice

Chapter 15

Assessing the effect of human factors in healthcare cyber security practice: An empirical study

Prosper Kandabongee Yeng ; Muhammad Ali Fauzi ; Bian Yang

Abstract

In recent times, the human element plays a major role in the surge of data breaches in healthcare. As a result, we hypothesized that there are gaps between the information security (IS) practices of the healthcare staff and the security policies. We further opined that if there are gaps, the causes could be culminating from poor work factors, personality, psychological, social and cultural perception issues. As a result, a survey was conducted with three departments in a typical hospital to assess a broad range of these factors. From the study results, the healthcare staff' IS knowledge and their self reported IS conscious care behaviour (ISCCB) showed a gap in their security practices. About half of the respondents' responses were in a higher risk region. In exploring for the reasons for these gaps, Workload showed a negative significant correlation (r=-0.346, p-value= 0.05) with information security-conscious care behaviour(ISCCB) risk and perceived barrier risk (r=-.363, pvalue=0.05). But, the hospital information security culture showed negative significant correlation with perceived vulnerability (r=-0.316, pvalue= 0.05), cues to action (r=-0.508,pvalue=0.01), and punishment severity (r=-0.425, pvalue=0.05). Based on the findings of this study, some intrinsic and extrinsic motivational factors can be explored to improve the security perceptions, and security culture of the hospital if causality is established.

15.1 Introduction

According to a recent data breaches report from Verizon, 83% of the cyber security incidents were caused by human elements [25]. This suggests that

the human element remains the top target for adversaries to explore and gain unauthorised access to information technology systems.

Healthcare is one of the targeted sectors by cybercriminals due to its richness in data [12], critical use-case and its multiple access points[14]. Also, healthcare data has a higher value on the dark web [21] and it is believed the sector has the financial muscles to pay for cyber criminals' attacks such as ransomware [14]. Recent instances include the German hospital hacks [13] which resulted in the death of a patient and the unauthorised access of some medical records in Finland [22] in which the hackers selfishly demanded ransoms from each of the patients involved. Even though the mode of ingress was not clear in these incidents, most of these attacks are as a result of the human elements.

To this end, fortification of the healthcare staff, otherwise called the human firewall, is deemed essential, to complement the technical information security (IS) solutions. Recognising the significant contribution of human factors in cyber security incidents, various researches have been conducted in this direction [15, 4, 4, 2, 24] however, these studies were incomprehensive [27]. In this paper, the gap between the healthcare security practices and their required security practices (specified in the Information Security policy) were assessed. Possible reasons for the gaps or the risky security practices were also explored. Specifically, we assessed individual differences, work factors, perception and organisational IS culture in relation to cyber security knowledge (K), attitude (A) and behaviour (B) termed in this work as the KAB risk variables. The significant contribution of this work is the adoption of the broad constructs for a holistic assessment of the human element in security practice.

15.1.1 Security practice and KAB

Information security practices are actionable measures that are taken by the healthcare staff to comply with the security policies or rules towards fulfilling the confidentiality, integrity and availability (CIA) of the information system[28, 26, 27]. There are various measures in security practices but the commonest include internet use, email use, social media use, password management, incident reporting, information handling and mobile computing[18]. These security practices were identified to be more prone to security violations within the context of the human aspect of information security practices. The compliance of these healthcare staff security measures depends on various factors including knowledge (K), attitude (A), and behaviour (B) termed as KAB variables. In addition to the KAB risk variables, we assessed the perceived risks.

Perception constructs such as perceived vulnerability(PV), Cues to action (CA), response efficacy(RE), self-efficacy(SE), punishment severity(SE), social bonding (SB) and perceived barriers (PB) were selected from vari-

ous theories including Health Belief Model (HBM), Protection Motivation Theory, (PMT), Theory of Planned Behaviour (TPB) and Social Control (SC) theory as a comprehensive perception variables in the aspect of human behaviour. HBM [19] was conceptually developed to assess for the motivations of which people do not engage (or engage) in healthy behaviours.

Furthermore, personality was included as one of the constructs [28] in this work. Personality traits reflects an individual's consistency and stability of his or her inherent characteristics of thoughts, feelings and behaviours. In comparison with other factors such as attitude, personality has various advantages including stability[17, 18], presence and generalisation [3] and are used to predict a longer-term behavioural pattern. The dimension of personality traits termed as the big five are extroversion (sociability, activity, assertiveness and positive emotional persons), agreeableness (trust and modesty), conscientiousness (goal-oriented persons), neuroticism (anxious, nervous, sad and tense persons) and openness(opened minded persons with experimental life).

15.1.2 Security Culture

Information security culture in an organization can be defined as the way and manner in which information security is practised in the organization [17]. These are the unwritten rules, knowledge, attitude, way of life and assumptions of how IS security measures are carried out in the organisation[16]. Just as organisational culture varies across different organisations, every hospital also has its aspect of security practices that are followed and integrated into their work life. But the concern is to assess to know whether the hospital's security culture is in line with good security practices.

15.1.3 Study objectives and hypotheses

It is often said that "an unexamined life is not worth living"; therefore, the goal of this study was to comprehensively assess the information security practice of a typical hospital among the healthcare staff in the area of human factors. The essence was to determine if there are IS compliance gaps by the healthcare workers and further process these gaps for possible reasons why they exist. Incentive measures could subsequently be explored to promote the positive factors while constraining the negative factors to enhance sound security practice. To meet this intention, the following hypotheses were developed:

- H1: Healthcare workers generally fail to entirely comply with security practices in terms of KAB.
- H2: Poor Work factors such as high workload, high work emergency and poor hospital security culture have adverse effects on knowledge,

attitude and self-reported information security-conscious care behaviour (ISCCB) risk.

- H3: IS Knowledge (ISK) risk, and IS Attitude (ISA) risk are predictors of self-reported information security-conscious care behaviour (ISCCB) risk.
- H4: Personality attributes of extroversion, agreeableness, conscientiousness, neuroticism and openness are predictors of KAB risk variables.
- H5: Personality attributes, poor Work factors such as high workload, high work emergency and poor hospital security culture have an adverse effect on IS perception variables such as perceived vulnerability (PV), cues to action (CA), response efficacy (RE), self-efficacy (SE), punishment severity (PS), social bonding (SB) and perceived barriers(PB)

15.2 Method

A total of 44 healthcare staff, took part in the online survey but 42 participants' properly completed their responses. The study took place in Norway in medical, surgical and emergency departments but due to ethical concerns, we are unable to disclose the name of the specific hospital. The questionnaire items included demographic data, workload and work emergency items, psychological and social-cultural perception items on security practices. The security practice items were asked to assess the knowledge, attitude and behaviour (KAB) risk of the participants. The risks of the security practices of the KAB variables and perception were calculated by averaging the related construct response items. The responses were formatted to mean that higher values represented higher risks while lower values represented lower risk in the KAB related questionnaire items. Some existing questionnaires were adapted [2] and a short version of personality questionnaire [6], representing the big five factors were used.

15.3 Results and discussion

A higher proportion of females(85.7%) took part in the study as compared to males (14.3%). This is quite reasonable due to the higher female to male nurse ratio in Norway [5]. The age ranges of the participants were between 21 to 60 years, of which 33.3% (the highest proportion) were within the age range of 31-40 years. In terms of positrons, half of the participants were nurses (50%) followed by doctors(33.3%), and physiotherapy (6%). The level of staff who responded to the questionnaire were basically operational staff

and managers/supervisors. Additionally, almost all of the respondents had more than 1-year of experience. Essentially, a high proportion of the respondents (88.1%) also had IS policy awareness.

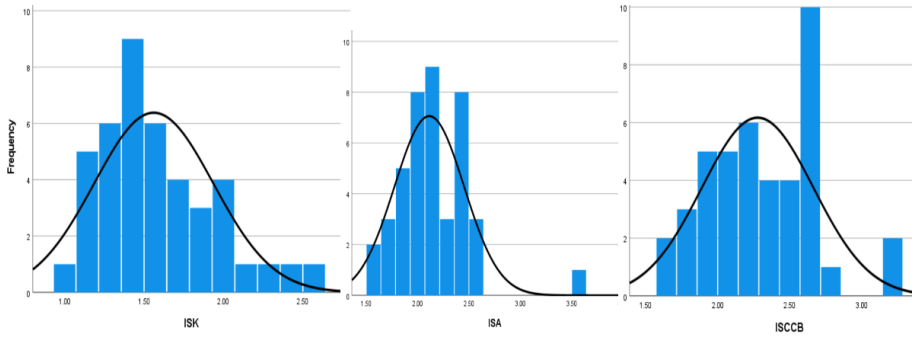


Figure 15.1: Distribution of information security risk KABs

From Figure 15.1 and Table 15.1, security compliance gaps were identified as some of the responses were skewed to higher risk regions. For instance, the security behaviour (ISCCB) skewness value (0.34) was fairly symmetrical (skewness between -0.5 t0 0.5), meaning that, a nearly equal proportion of the responses were in both low and high-risk regions [10]. With positive skewness of 0.9 in IS behaviour knowledge risk, there was moderate skewness (between -1 and – 0.5 or between 0.5 and 1). The IS attitude recorded a highly skewed (skewness less than -1 or greater than 1) positive response of 1.536. However, from figure 15.1 of ISA and that of ISCCD, all responses were in the higher risk region of security practices. Following these gaps as hypothesized in (H1), further analysis was conducted as defined in the other hypotheses.

With reference to table 15.2, the study showed that workload has a negative significant correlation (r=-0.346, p-value= 0.05) with information security-conscious care behaviour(ISCCB) risk. Furthermore, as specified in H3, ISCCB risk has a positive correlation with both information security knowledge risk (ISK) and information security attitude (ISK) of (r= .575,pvalue = 0.01) and (r = 0.654, pvalue = 0.01) respectively. Additionally, ISK and ISA risks showed a positive significant correlation of r = 0.549 and pvalue = 0.01. Furthermore, the hospital IS culture negatively correlated with both the risk of ISA and ISCCB at significant levels of (r = -.447, pvalue = 0.01) and (r = -.525, pvalue=0.01) respectively. The negative correlation between workload and ISCCB risk interprets that as workload increases, the risk of ISCCB also decreases rather. This does not suggest causalities among these variables however, related studies such as [11], contradicts these findings.

It was found in the study that workload has a positive correlation with

Table 15.1: Skewness of KAB variables

Statistics		ISCCB	ISK	ISA
N	Valid	42	42	42
	Missing	0	0	0
Mean		2.2772	1.5612	2.1139
Median		2.2500	1.4643	2.0714
Std. Deviation		.38778	.37518	.33911
Skewness		.341	.921	1.536
Std. Error of Skewness		.365	.365	.365
Kurtosis		-.372	.330	5.581
Std. Error of Kurtosis		.717	.717	.717

Table 15.2: Correlation of work factors and security behaviour

	Workload	Work emergency	Hospital IS Culture	ISCCB	ISK	ISA
Workload	–					
WorkEmergency	.518**	–				
Hospital_IS_Culture	0.211	0.045	–			
Behaviour Risk	-.346*	0.019	-.525**	–		
Knowledge Risk	-0.081	-0.056	-0.297	.575**	–	
Attitude Risk	-0.065	-0.020	-.447**	.654**	.549**	–

*p ¡ 0.05; **p ¡ 0.01.

phishing susceptibility clicks. Based on their findings, the authors suggested a balanced workload for healthcare staff to enhance effective cyber security practice. This is in contradiction with this study, suggesting further study in this direction. With regards to information security knowledge and attitude risks, in relation to ISCCB risk, the positive correlation is interpreted to suggest that poor IS knowledge and attitude translate into risky ISCCB and verse versa. To this end, healthcare facility management would adapt to ways of increasing knowledge of information security among healthcare workers to enhance a positive attitude towards information security practices. Furthermore, personality and security knowledge, attitude and behaviour were assessed in response to H4. The results showed a negative significant correlation (-.317, pvalue=0.05) between extroversion and ISA. This suggests that extroversion is a predictor of ISA risks. As attitude is known to be a predictor of behaviour [16], the effect of IS security attitude on ISCCB was realised, as extroversion showed a negative correlation with ISCCB risks. With negative correlation, it interprets that extrovert personality correlates with lower risk of IS attitude which might therefore have a relatively insignificant effect on lower risks of IS knowledge and behaviour. This is because this study(as shown in table 15.2 and other studies [18, 16, 20] showed that a good attitude is a positive predictor of both knowledge and

cyber security behaviour.

Additionally, a related study [7], also showed that extroversion is a predictor of cyber security behaviour. This supports the view that outgoing people have a good attitude towards security practices in which the indirect effect can be translated into good security behaviour. But in contrast to our findings, a study [8] showed that conscientiousness rather predicted cyber security behaviour but not extroversion. This suggests that these findings need to be contextualised within the study scope.

Work Factors, Personality and Psycho-social-cultural perceptions were assessed as specified in (H5) and shown in table15.3.The analysis showed that workload has a negative correlation with perceived barriers, however, work emergency showed no significant correlation with any of the perception variables. Furthermore, Hospital information security culture showed negative significant correlation with the risks of perceived vulnerability (r=-0.316, pvalue= 0.05), cues to action (r=-0.508,pvalue=0.01), and punishment severity (r=-0.425, pvalue=0.05).

Table 15.3: Correlation of work factors and security behaviour

	Workload	Work Emergency	Hospital IS Culture	PV	CA	RE	SE	PS	SB	PB
Workload	–									
Work Emergency	.518**	–								
Hospital IS Culture	0.211	0.045	–							
PV	-0.064	-0.092	-.316*	–						
CA	-0.204	0.040	-0.243	0.174	–					
RE	-0.045	-0.067	-.508**	.356*	0.198	–				
SE	-0.040	0.105	-0.025	0.043	.351*	-0.008	–			
PS	-0.139	0.047	-.425**	0.296	0.258	0.195	-0.021	–		
SB	0.001	0.062	-0.198	.348*	.346*	0.164	0.244	.435**	–	
PB	-.363*	-0.023	-0.225	0.130	0.095	-0.084	0.196	.311*	0.180	–

*p <0.005; **p <0.01.

The findings indicate that a higher workload predicts lower security risk behaviour with regard to perceived barriers(PB). This is in contrast with the H5 as we thought a higher workload will influence poor IS security practices among the perception variables. In this hospital, it is a possibility that the healthcare staff are not driven by the workload burden to have poor IS perceived barrier effect. Unfortunately, there are no studies that examined workload and PB. This calls for further studies in this area to provide more meaning to these findings. Meanwhile, hospital information security culture is a predictor of low risk of cues to action(CA) risk, response efficacy(RE) risk, and punishment severity (PS) risk, in this survey, suggesting that good IS culture can result in low-security perceptions in RE, PS and CA. In fact, the effect of organizational security culture on conscious care security practice has been widely acknowledged[1, 23, 4] which is in line with the correlation of security culture in this hospital and the risks of security perceptions in RE, PS and CA.

15.4 Conclusion And study implication

Following the need to enhance better cyber-security practice in healthcare, this study correlated a broad range of human factors and work-related factors in a typical hospital. The purpose was to assess for possible gaps in information security practice among healthcare workers and their related possible causes. The study showed that workload has a negative significant correlation (r=-0.346, p-value= 0.05) with information security-conscious care behaviour(ISCCB) risk and perceived barrier risk (r=-.363, pvalue=0.05). Additionally, a negative significant correlation between extroverted and ISA was observed. Furthermore, hospital information security culture showed negative significant correlation with perceived vulnerability (r=-0.316, pvalue= 0.05), cues to action (r=-0.508,pvalue=0.01), and punishment severity (r=-0.425, pvalue=0.05).

Based on these findings, the hospital management can improve the conscious care security practice of the hospital's staff by using the appropriate incentive measures. For example, as the study showed IS hospital culture to be a predictor of perceived vulnerability and punishment severity, intrinsic and extrinsic incentives [9] can be adopted to influence staff security behaviour. Additionally, other incentives can be used to promote introversion to advertently promote conscious care security practice. With regards to workload and work emergencies, further studies need to be conducted with regards to the effect on security practice. Because our results in this study contradict other previous findings, provoking thorough studies for new knowledge. Our hypothesis was that high workload and work emergency in healthcare would impede sound IS security practice. But with regards to workload, the results indicated the reverse. It is possible that the culture at the healthcare facility influences staff to perceive that, amidst workload, and barriers, security practice rather increases.

Our study was limited by a few participants (thus, 42) healthcare workers who took part in the study. This makes it difficult to effectively generalise the study but limits the study implications to the three departments that took part in the study. Besides, bias from self-reported behaviour can not be discounted. These are reemphasizing the need to conduct further studies by observing directly how healthcare staff carry out security practice coupled with interviews to have a better understanding of these findings.

15.5 Bibliography

[1] ALFAWAZ, S., NELSON, K., AND MOHANNAK, K. Information security culture: a behaviour compliance conceptual framework. In *Information Security 2010: AISC'10 Proceedings of the Eighth Australasian Conference on Information Security [Conferences in Research and Practice in Information*

Technology, Volume 105] (CRPIT, 105. Boyd, C. and Susilo, W. Eds., ACS. 47-55, 2010), Australian Computer Society, AISC, pp. 51–60. 447

[2] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., AND XU, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. 272, 274, 296, 313, 404, 406, 412, 414, 442, 444, 457, 512

[3] DIGMAN, J. M. Personality structure: Emergence of the five-factor model. *Annual review of psychology 41*, 1 (1990), 417–440. 443

[4] DONG, K., ALI, R. F., DOMINIC, P., AND ALI, S. E. A. The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability 13*, 5 (2021), 2800. 442, 447

[5] ERIKSEN, W., AND EINARSEN, S. Gender minority as a risk factor of exposure to bullying at work: The case of male assistant nurses. *European journal of work and organizational psychology 13*, 4 (2004), 473–492. 444

[6] GOSLING, S. D., RENTFROW, P. J., AND SWANN JR, W. B. A very brief measure of the big-five personality domains. *Journal of Research in personality 37*, 6 (2003), 504–528. 413, 414, 415, 444, 499, 501, 502

[7] GRATIAN, M., BANDI, S., CUKIER, M., DYKSTRA, J., AND GINTHER, A. Correlating human traits and cyber security behavior intentions. *Computers & Security 73* (2018), 345–358. Available from: https://www.sciencedirect.com/science/article/pii/S0167404817302523. 447

[8] HALEVI, T., MEMON, N., LEWIS, J., KUMARAGURU, P., ARORA, S., DAGAR, N., ALOUL, F., AND CHEN, J. Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-Based Applications and Services* (New York, NY, USA, 2016), iiWAS '16, Association for Computing Machinery, p. 318–324. Available from: https://doi.org/10.1145/3011141.3011165. 447

[9] HERATH, T., AND RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems 47*, 2 (2009), 154–165. 7, 405, 412, 428, 448, 457, 493

[10] HO, A. D., AND YU, C. C. Descriptive statistics for modern test score distributions: Skewness, kurtosis, discreteness, and ceiling effects. *Educational and Psychological Measurement 75*, 3 (2015), 365–388. 445

[11] JALALI, M. S., BRUCKES, M., WESTMATTELMANN, D., AND SCHEWE, G. Why employees (still) click on phishing links: investigation in hospitals. *Journal of medical Internet research 22*, 1 (2020), e16775. 11, 15, 272, 273, 274, 280, 282, 284, 285, 295, 296, 297, 299, 312, 313, 445, 491, 492, 508

[12] KLICK, J., KOCH, R., AND BRANDSTETTER, T. Epidemic? the attack surface of german hospitals during the covid-19 pandemic. In *2021 13th International Conference on Cyber Conflict (CyCon)* (Alpha Strike Labs, Berlin, Germany, 2021), no. 20778688, IEEE, pp. 73–94. 442

[13] NEWS, A. German hospital hacked, patient taken to another city dies, September 2020. Available from: `https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94`. 442

[14] NEWS, B. S. H. I. Ransomware is leading hospital boards to pour more money into cybersecurity, October 2021. Available from: `https://www.healthcareitnews.com/news/ransomware-leading-hospital-boards-pour-more-money-cybersecurity`. 270, 442

[15] NG, B.-Y., KANKANHALLI, A., AND XU, Y. C. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 4 (2009), 815–825. 9, 271, 272, 273, 296, 313, 442, 496, 509, 512

[16] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., AND ZWAANS, T. The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security 66* (2017), 40–51. 10, 278, 404, 405, 406, 408, 413, 414, 415, 426, 428, 443, 446, 499, 501, 502

[17] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., AND FERGUSON, L. Human factors and information security: individual, culture and security environment. Tech. rep., DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) COMMAND . . . , 2010. 443

[18] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. The development of the human aspects of information security questionnaire (hais-q). 7, 10, 278, 282, 414, 442, 443, 446, 461, 498

[19] ROSENSTOCK, I. M. The health belief model and preventive health behavior. *Health education monographs 2*, 4 (1974), 354–386. 412, 443

[20] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 9, 10, 12, 15, 200, 274, 405, 407, 412, 428, 446, 457

[21] SEH, A. H., ZAROUR, M., ALENEZI, M., SARKAR, A. K., AGRAWAL, A., KUMAR, R., AND AHMAD KHAN, R. Healthcare data breaches: Insights and implications. In *Healthcare* (Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, India, 2020), vol. 8, Multidisciplinary Digital Publishing Institute, Healthcare MDPI, p. 133. 442

[22] SIPILÄ, J. Patients in finland blackmailed after therapy records were stolen by hackers, September 2020. Available from: `https://edition.cnn.com/2020/10/27/tech/finland-therapy-patients-blackmailed-data-breach-intl/index.html`. 442

[23] TENZIN, S. *An investigation of the factors that influence information security culture in government organisations in Bhutan*. Ph.D. thesis, Murdoch University, 2021. 447

[24] UFFEN, J., GUHR, N., AND BREITNER, M. H. Personality traits and information security management: An empirical study of information security executives. 10, 410, 442

[25] VERIZON2021. 2021 data breach investigations report, November 2021. Available from: `https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf`. 1, 270, 293, 441, 454

[26] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[27] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (2019), IEEE, pp. 3242–3251. 11, 15, 22, 138, 200, 217, 224, 236, 273, 274, 404, 406, 407, 409, 414, 426, 442, 491, 498

[28] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 1, 2, 6, 10, 11, 15, 17, 23, 199, 217, 224, 274, 282, 404, 405, 406, 407, 409, 410, 414, 442, 443, 454, 457, 491, 498

2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)
https://doi.org/10.1109/IOTSMS58070.2022.10061936

Chapter 16

Assessing cyber-security compliance level in paperless hospitals: An ethnographic approach

Prosper Kandabongee Yeng ; Bian Yang; Monica Stolt Pedersen

Abstract

Digitalization in healthcare can be a double-edged sword. Whiles, it transforms the efficiency of healthcare operations through the use of IT infrastructure, its security and privacy concerns can be life-threatening, thus threatening the very lives that healthcare exists to safeguard. Motivated by this, we combined focus-group discussion and observational methods to assess the cyber security situations in two hospitals that have migrated to paperless systems in Ghana. Paperless systems are the adoption of electronic health record (EHR) systems by hospitals, and they are usually hosted within a healthcare IT infrastructure. This is one of the few studies that has used the ethnographic investigation method to unearth the nature of security and privacy practice in hospitals with the, aim to enhance security practices in healthcare. The findings revealed that participants understood various areas of security practice knowledge, however, that did not translate into their security behaviour as a variety of security gaps were identified. System misuse, Security and privacy violations, characterised by password sharing, authentication sharing, unauthorised access to patient information and physical security issues were associated with the security practice of the healthcare staff. The causes of these security malpractices were discussed to include a variety of factors such as peer pressure, bad moral conduct (eg personal gain), work factors and security development issues. Based on the assessment, practical implications were therefore suggested to the hospitals. Hospitals that are migrating to paperless systems were also advised to establish the fundamental security structures such as security policy establishment and the right security personnel to averse such security menace.

16.1 Introduction

In recent times, security and privacy issues in healthcare have been reported at alarming rates. For instance, in 2021, the National Health Service (NHS) in the UK was targeted with 357 million malicious emails [13]. About 3,996 staff received these emails of which an average of 89,353 were targeted at each employee. Additionally, within the COVID-19 period, phishing attack was largely reported to have largely increased in healthcare within a range of 600% to 9000% [28, 33, 9]. Aside from these external threats, healthcare personnel has recently been reported to be snooped in the records of 145 patients, who were her friends and acquaintances in a typical hospital in Norway. In this incident, the chief executive officer of the hospital feared losing patients' confidence [12]. All these are security and privacy incidents originating from the human element.

The human aspect of information security has been reported to contribute to about 85% of security breaches of which the healthcare sector is one of the most targeted sectors [34, 35].

The human factors in security practice relate to the reliance on the desecration of human users to comply with the organizational security measures and policies in order to enhance the CIA. For instance, the access control clause of ISO 27002 requires users to neither share their passwords nor share their authenticated session with unauthorised users [17]. Other human-centred security practices include software updates, avoidance of suspicious emails and the use of strong passwords [18, 6, 3]. Human-centred security practices are much required to complement technological countermeasures such as firewalls, intrusion detection and prevention systems, security policy configurations and antivirus systems, in the mobilization of security countermeasures in combat against security incidents [27]. However, the reliance on healthcare staff to observe security and privacy measures can not be guaranteed [40]. First, due to individual, psychological, social and cultural factors, coupled with work-related and organizational factors, security controls that are reliant on the human element may fail. Secondly, as humans are deemed the weakest link in the security chain, cyber-criminals tend to exploit that through various ways including psychological manipulations, and that can lead to data breaches. The adverse impact of security and privacy breaches in healthcare can be enormous. One of the worst-case scenarios is when a woman was reported to have died due to delayed treatment, caused by a ransomware attack on the hospital in Germany, in which she was to be treated [23] . Aside from these, healthcare organizations that fail to comply with regulations could also be fined up to Twenty Million Euros [7] in the European Union.

A lot of efforts have been concentrated in transforming cyber security practice in the aspect of human behaviour in healthcare. While these studies significantly contributed to the fortification of the "human firewall", quan-

titative approaches have largely been adopted. Meanwhile, users such as healthcare workers have subtle variant behaviour in the usage of ICT systems in healthcare that can increase susceptibility and attack surfaces in healthcare systems [31]. Fortunately, adopting a qualitative approach in assessing people with nuanced behaviour has been noticed to provide fine grain results, communicating the richness of the knowledge of the studies for better measures [21, 20]. Hence the general objective of this paper was to use qualitative means to explore the level of cyber security compliance among healthcare staff in hospitals that have adopted Electronic Health Record (EHR) systems, termed as paperless or folder-less systems in Ghana. The aggregated results could guide in designing effective incentives towards improving the performance of security practices to meet health organizations' business objectives. The specific objectives are to find answers to the following research questions: 1. What do healthcare workers know about and practice on cyber security requirements in the hospital? 2. How do healthcare staff perceive cyber security in relation to their work? 3. What are the cyber security experiences of healthcare workers in their effort of balancing therapeutic functions while observing security measures? 4. What factors influence security compliance among healthcare staff? 5. What motivates the staff to comply with security measures?

16.2 Background and related work

Healthcare security practice analysis, modelling and incentivization (HSPAMI), is a project being operated by the centre for cyber and information security of the Norwegian University of Science and Technology (NTNU) and is funded by the ministry of health and care of Norway. One of its goals is to comprehensively assess human factors in relation to security practice, such as work factors, individual factors, and psychological, social and cultural practice (PSCP) of healthcare staff. The purpose is towards assessing security gaps that will lead to developing incentive schemes towards improving the CIA in healthcare infrastructure. In that vein, a qualitative study was conducted in two medium-sized hospitals that fully adopted electronic health record (EHR) systems called paperless systems. Amidst the massive adoption and roll-out of EHR systems in tertiary level hospitals such as regional hospitals and secondary/primary hospitals including district-level health facilities, it is crucial to reflect on the security behaviour of the end users who are herein known as the healthcare staff. In our previous work, a quantitative approach was used to survey for the intended security practice among these healthcare staff [38]. However, in order to have a deeper and better understanding of the security situation in relation to the healthcare staff security practice, a focused group interview was adopted in this study, in complement of our quantitative study, to showcase the reasons,

opinions, experience and motivations of the different kinds of security related behaviour among healthcare staff [25]. For instance, in the survey of [38], work emergencies, information security knowledge risks, and information security attitude risks were identified to be significantly correlated with the self-reported information security-conscious care behaviour risks of the participants. However, the reasons for these security gaps could not be concretely explained from the quantitative findings. Related research findings reasoned in this direction but having reviewed them in section 16.2.2, certain gaps were identified in comparison with our objective.

16.2.1 Theoretical background

In observing security practices in a typical hospital, areas of concern that are a potential threat to the CIA are often observed [36]. The observational areas that were adopted in this study include but are not limited to access control, authorization, authentication and backup [16]. Authentication is a structured way to ensure that only authorized or approved users access the appropriate data and files in the hospital's IT infrastructure. Authorization mechanisms is to ensure that a user has permission to access an object. Access control involves ways of controlling who should access an object and the techniques often used are password use, biometric scans, PINS and security tokens.

Aside from these technical observational areas, psychological, social and cultural theories were used to observe the security practice of the human elements. These theories include the health belief model (HBM), protection motivation theory (PMT), and social control (SC). HBM was originally developed to predict healthcare behaviour among individuals. It has the following constructs;

- perceived vulnerability (PV) is the perception of being susceptible to a security threat or a cyber attack while PS is the perception of the consequence of the attack.
- perceived severity (PS), is one's perception of the severity of the impact of the related security breaches.
- perceived benefit(PBf) is the perception of the available opportunities of the recommended course of action.
- perceived barriers (PB) are the perceived obstacles associated with observing the security practice.
- cues to action (CA) stimulates one to adapt to the recommended solution.

- self-efficacy (SE) is the appraisal of one's ability to comply with the recommended solutions.

Also, PMT consists of threat and coping appraisals that are used by individuals in decision-making during stressful or harmful circumstances [24, 15, 40]. Psychological, social, and cultural perception has therefore been widely used in the quantitative assessment in cyber security practice[29, 14, 4], but not in the ethnographic context. We, therefore, opine in this work that assessing security practice by combining the technical observational measures as specified in [36, 16] and the psychological, social and cultural factors as specified in [39] could be an efficient approach towards revealing novel results of security practice among the healthcare staff.

16.2.2 Related work

In an effort to mitigate security issues, Renaud et al., interviewed healthcare staff of the National Health Service (NHS) in the United Kingdom (UK) to determine their experience and perception of information security policy [27]. An interpretative phenomenological analysis (IPA) approach was adopted in this study where the healthcare staff were interviewed individually. The study discovered that the staff felt subdued by the IS policy. Additionally, the staff experienced a lack of support in compliance, at the same time, they were being compelled to follow the security policies. Better policy compliance measures were therefore proposed based on the study. These include setting up an incident response team, recognition and reward scheme for secure behaviour. Similarly, Gebrasilase et al. investigated factors that affect the implementation of security culture at Hawassa Referral hospital in Ethiopia [8]. The study model consists of areas including knowledge, attitude, belief and actions of healthcare staff and medical students in relation to information security behaviour. Through an in-depth interview, the authors concluded that having a security policy alone does not translate into information system security compliance. So both long-term and short-term recommendations were provided to enhance security compliance. In these studies, [27, 8] better ways of enhancing security practices were suggested. However, the IPA approach (adopted by Renaud et al) objective is to deeply explore personal lived experience while a focused group (which is to be used in this research work) engages a group of participants in a discussion of the topics. Comparatively, a focused group aim to ignite a conversation in order for the participants to learn and be reminded of the discussion [22].

In related work, Hassan et al interviewed 19 healthcare professionals to understand the factors that influence IS culture in healthcare [11]. The healthcare staff categories that were interviewed include pharmacist, nurse, doctor and IT admin. Twelve themes were eventually developed from the study. These include security knowledge, security awareness, security be-

haviour and security policy. The authors concluded that top management needs to instil the habit of security knowledge, awareness and behaviour in healthcare staff as these three themes were deemed to be the key findings. Alumaran et al., research the role and influence of culture in complying with information security in Saudi Arabia health service [2]. A mixed method was also adopted in this paper where a semi-structured interview questionnaire was distributed among healthcare workers in three hospitals. Six cultural dimensions were identified in the qualitative analysis. These include national culture, leadership, thrust, technology, multicultural interaction and job roles of employees. While these papers identified IS policy compliance issues in healthcare in relation, some of the perception constructs relating to health belief models or protection motivation theories including perceived vulnerability, and perceived severity was not explored. Additionally, work factors such as workload and work emergencies were not in the scope of these studies. To this end, this study focused to holistically understanding the compliance of security practice of healthcare staff in paperless hospitals.

16.3 Method

16.3.0.1 Study design

A focused-group discussion and shadow observations were adopted in this study, to explore the compliance level of cybersecurity practice among the healthcare staff. Ethical approval was obtained from the Kintampo Health Research Center (KHRC) Scientific research committee (SRC) in Ghana. Following that focus groups consisting of IT staff, operational staff, and top management were formed. The focus group was used because of group dynamics, and the need for participants to freely express their experiences and opinions [10]. Thematic analysis was used to analyse the interview transcripts.

16.3.0.2 Context and setting

Healthcare facilities such as hospitals, health centres and clinics are shifting from paper-based record management systems to EHR systems commonly known as paperless systems. Meanwhile, cyber security relating to the human element has been a major problem for many organizations including healthcare. In view of this, a focus group interview was conducted in two hospitals in Ghana to understand the security compliance level towards improving the CIA of the healthcare systems. Based on security and ethical concerns, the names of these hospitals have been pseudonymized in this paper with hospitals A and B.

16.3.1 Participants

A written research invitation letter was shared with hospitals that adopted paperless systems in two regions in Ghana, through convenience sampling [30]. A description of the research and how it was to be conducted were detailed in the letter. Two healthcare facilities, known in this work as A and B, agreed to join the study. The staff strength was 310 and 323 respectively. These facilities were located in large communities with populations of about 106,0000 and 193,000 for hospitals A and B respectively [1]. Essentially, these were medium size hospitals that represented all hospitals in this region. Even though, the sample of the hospitals did not represent tertiary-level facilities such as the regional hospitals, the sample, represented the majority of health facilities, thus the medium size hospitals.

Consent forms, the research objective and the interview schedule were shared with the hospital staff in July 2021. Participants who consented to the study through written and verbal mode submitted their signed consent forms on the dates of the interviews in August 2021.

16.3.1.1 Data collection and analysis

For each of the hospitals, three focused groups including the IT group, the operation group and the Administrative group (i.e. the leaders) were formed as shown in Table18.1. For each of interview discussion, a short presentation about the objective of the study and the interview process preceded the discussion. Participants were also informed that the study was voluntary and anonymous. Therefore, those who duly consented took part in the study.

A semi-structured interview guide with open questions was used in this study. The areas of the questions include assessing the knowledge of security practices of the participants, their experience while complying with security practices, and their perception of cyber security in their hospitals. Additionally, the factors influencing cyber security practices, and incentives toward security compliance were also discussed in the interview discussion.

Each focused-group discussion took about one hour. The interview was audio-recorded and later transcribed. The transcription was verified by one of the authors. Following that the six transcribed files which were Microsoft word files, were analysed with NVivo release 1.6.1 (1137). Each of the files was then coded and categorised. The categories were then grouped into themes and the key points in each of the categories were identified as shown in Table 16.2. Discrepancies in the categorizations were resolved through objective discussion among authors.

Table 16.1: Participants demographics

Study ID	Gender	Role	Facility	Group
001	Male	IT Manger	A	IT
002	Male	Assistant IT Manger	A	IT
001	Male	Bio-statistician	A	Operation staff
002	Female	Head of records	A	Operation staff
003	Female	Nurse	A	Operation staff
004	MAle	Doctor	A	Operation staff
005	Female	Nurse Precriber	A	Operation staff
006	Female	Accountant	A	Operation staff
007	Male	Doctor	A	Operation staff
008	Male	Nurse	A	Operation staff
009	Female	Insurance claims officer	A	Operation staff
001	Female	Admin, Head of hospital	A	Admin
002	Female	Head of Nurses	A	Admin
001	Male	Head of IT	B	IT
002	Female	IT officer	B	IT
003	Male	IT officer	B	IT
001	Female	Human resource	B	Admin
002	Male	Doctor	B	Admin
003	Male	Medical assistant	B	Operation staff
004	Female	Nurse	B	Operation staff
005	Male	Lab technician	B	Operation staff
006	Female	Theatre nurse	B	Operation staff
007	Female	Emergency nurse	B	Operation staff
008	Female	Record officer	B	Operation staff
009	Male	Pharmacist	B	Operation staff
010	Female	Doctor	B	Operation staff
011	Female	Maternity nurse	B	Operation staff
012	Female	Nurse in charge	B	Operation staff

Table 16.2: Emerged categories and key findings

#	Interview guide area	Themes	Number of themes	Key findings
1	Knowledge and practice of security measures	Password use, access control, data backup, virus control, training, session control, security governance, vulnerability reporting and logging	9	Gap in the use of reliable security policy
2	Security and privacy experience	System misuse, security violations, privacy violations, physical security issues, security design issues, data integrity and security	7	security and privacy violation through password sharing and active accounts of users who are no longer staff of the organization
3	Factors that influence security and privacy practice	Work factors, the moral conduct of users, low management support, usability and resource constraints	5	Work emergency and moral conduct threatens huge security issues
4	Security perception	Perceive vulnerability, Perceived severity, Perceived efficacy	3	Users fear for implications on patients in the event of system compromise
5	Mitigation and incentive strategies	Social control, training, management action and response, enhancing privacy and security control in an EHR system, providing support to users	5	Management require to adapt to a security policy that will enhance security while discouraging bad moral conduct

16.4 Analysis and findings

About 29 themes and their respective key findings emerged in the analysis. The identified themes, the interview guide questions, the number of themes and the key concerns or findings are shown in table 16.2.

These findings are further presented in their related interview guide areas in the following sections.

16.4.1 Knowledge and practice of security and privacy measures

In this interview guide question, the participants shared their knowledge on what they knew about their hospitals' cyber security and privacy measures. Security and privacy measures were explained to participants to relate to security practices or controls that have been provided in the hospital for staff to observe towards safe guiding confidentiality, integrity and availability (CIA). The aim was to assess the knowledge level of healthcare staff regarding security requirements since various studies suggested that the knowledge and the understanding of cyber security measures are significant to conscious care security behaviour [38, 26]. The participants, therefore, shared what they knew about security measures in their hospital. All the participants in the various groups shared their knowledge of security measures relating to password use, access control, vulnerability reporting

and logging of users' accesses. Additionally, the IT group and the admin group also shared their knowledge on security governance, virus control, data backup and training.

Regarding security governance, both hospitals A and B were not using approved security policies in operating their IT infrastructure. However, hospital A has a draft security policy. For instance, when hospital B was asked about the security policy of the hospital, the IT manager responded that "we do not have a written down policy but when an account is being created for a user, that user was usually informed not to never share their passwords". In the case of hospital, A, both the leader of the hospital (the hospital's administrator) and the IT manager who were in separate interview groups, attested that the hospital has a draft policy. On the aspect of password use, all the participating groups acknowledged the use of passwords as a security measure on their EHR system as shown in Table 16.2. The use of passwords was identified as the most popular known security measure among the participants. The latter were aware of password sharing as an unacceptable security practice. They were also conscious of password-changing practices and the need to disable passwords for unauthorized users.

16.4.2 Experience with cyber security compliance

The various interview groups (Admin group, Operation, and IT) shared their experience on cyber security in response to the interview guide concerning the "cyber security experience of participants in the hospital". Varying cyber security experiences themes that were shared are categorized into security violations, privacy violations, system misused, physical security issues, data integrity issues and security design issues as shown in Table 16.2.

Issues relating to security violations were identified to include password sharing, logout failures, authentication sharing, and system manipulation. For instance, on system manipulation, a participant (007) said that "it is not allowed for doctors to consult themselves when they are sick. However, close friends do exchange their EHR access credentials. So, when they are sick, they will then use the credentials of their friend or colleague to consult for themselves". On the recount of privacy violations, the IT and the operational staff of hospital A narrated their experiences including scenarios where staff can take patients' information with phones and share it with unauthorized persons. Regarding physical security, the IT department of hospital A reported several instances where laptops and patients' relatives' mobile phones have been stolen. A participant with the ID 002 of the IT department of Hospital A narrated two situations where the staff left laptop computers unprotected. Upon information, the human resource manager picked up the laptops and pretended that they were missing.

16.4.3 Factors that contribute to cyber security compliance

In this interview guide, factors that were identified to have contributed to these security gaps were categorized into work factors, the moral conduct of users, low management support, usable security, and resource constraints. Regarding moral conduct, issues of personal gains, peer pressure and other social influences were identified. For instance, a participant in the operational group (007) recounted a bad experience where one of his colleagues said he (007) was a difficult person after he declined to share his authenticated system with that colleague upon the request of the former. Furthermore, according to the IT staff, a higher workload is one of the factors that causes password sharing among healthcare staff. For instance, a participant (001) from the IT department of hospital A said "as you have observed, we are only two IT staff for this big hospital. So, sometimes when we are occupied, we give out the password of the hospital's access points to staff who are not supposed to have that". Additionally, a participant (002) of the IT department of hospital A said, "there have been two instances where I shared admin password with a user at the records department in the night." Furthermore, according to a management member (002) of hospital B, during emergencies, other staff tend to support the few experienced staff. This results in a situation where the experienced staff who have legitimate credentials, do share their passwords with their colleagues. It was added that sometimes too, the staff will inadvertently loudly mention out their password during an emergency, thereby, broadcasting it. Aside from these, it was observed that it is difficult to follow security practices especially when computers are during emergencies. According to an admin participant (002), of hospital A, some staff do not even use the EHR system during emergencies. They record the patients' information on pieces of paper, mostly with the intention to transfer to the EHR afterwards. This often leads to forgetfulness on the part of the staff to enter the patient's information into the system.

16.4.4 Security perception

In this interview guide question, participants were asked to describe how they feel about the cyber security situation in the hospital. Themes such as perceived vulnerability, perceived severity and perceived efficacy emerged in the discussion. A participant within the operations group (001), in hospital B, opined that "Unavailability of the system, such as downtime can cause needless death. For instance, if the system is down or slow before the patient gets to the consulting room, the condition might have deteriorated and the doctors may not be able to do much to bring the person back to life".

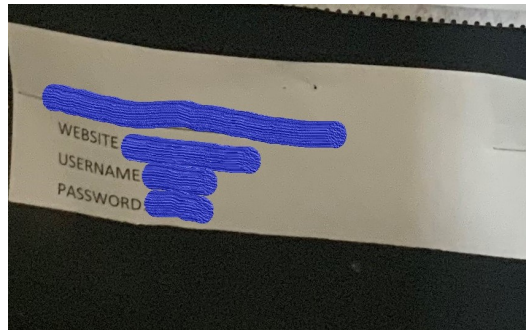


Figure 16.1: Displayed access credential on a noticed board

16.4.5 Mitigation strategy

With the aim to elucidate opinions towards enhancing cyber security practice in healthcare, mitigation and incentives were explored as part of the interview guide. The suggested methods by the participants for improving cyber security practice in healthcare were categorized into social control, training, management action and response, enhancing privacy and security controls in the EHR system and providing IT support to users as shown in Table 16.2.

On the aspect of social control, positive and negative reinforcement were suggested. For instance, a management member in hospital B suggested that "if someone is caught sharing their password, they need to be punished". Staff who are found to be complying with the security policy also need to be recognized for their effort. Another management member in hospital B indicated that "on the part of password sharing, serious training needs to be conducted". Others also suggested for staff to be educated on logout after using the EHR system, and mobile phone use. Participants also proposed for management to take action regarding disabling the passwords of staff who are no longer working with the hospital.

16.4.6 shadow observation at the hospitals

As shown in Figure18.1 , a user credential was displayed on a notice board. Additionally, some work areas were physically secured against unauthorised but at the same time, laptops which were logged on were not much protected against unauthorized users as seen in 16.2.

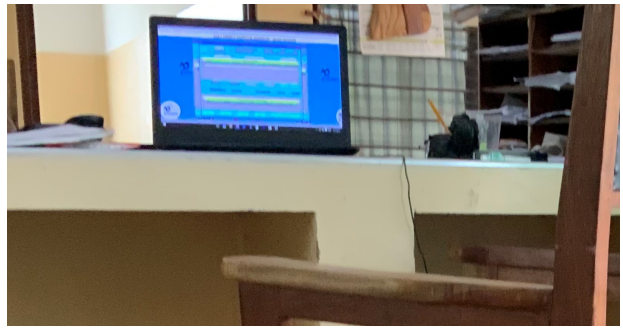


Figure 16.2: Unattended system without logout

16.5 Discussion

This study revealed some gaps in security practice and identified various factors that tend to thwart the efforts of sound security practices in hospitals. The key themes that were found include a lack of reliable security policies for governing the IT infrastructure of the hospitals, dominance of password violations (eg as shown in Figure 18.1) together with violations of other controls, the challenge of harassment and peer pressure to misuse security requirement compliance. Additionally, system manipulations and work emergency cases aggravate the sound cyber security practice in these hospitals.

In the context of legal requirements, governing a critical IT infrastructure, such as healthcare without an approved security policy can be tantamount to a lawless country [37]. In such a situation, every user or healthcare staff has the tendency to violate security requirements, thereby endangering patients' safety, security and privacy without being held accountable for their actions and inaction. According to a study that assessed legal aspects of information security in healthcare [37], a security policy is one of the security governance tools that serves as the law in the usage of the IT infrastructure. The major difference between law and security policy is that while ignorance of state law is not an acceptable excuse, ignorance of an organizational policy is an acceptable defence. This suggests that having a security policy is not even enough. It requires adequate training and acceptance by the users to abide by it before the policy can serve its intended legal purpose. Aside from the legal bases, the lack of security policy suggests that the organization does not have a comprehensive and structured catalogue of the security and privacy requirements, plans and measures for their IT infrastructure. For instance, an enterprise information security policy defines the entire scope, strategic direction, and goals of its organizational information needs [Whitman ME, Mattord HJ. Principles of Informa-

tion Security. 4th edition. Boston, MA, USA: Cengage Learning; 2011]. This directs the formulation and implementation of measures to safeguard the purpose of the IT infrastructure. Additionally, there are system-specific and issue-specific policies that are formulated towards enhancing confidentiality, integrity, and availability. Notwithstanding, the participants expressed their knowledge of other security practices and measures including password management logging, vulnerability reporting, physical security, access control, authorization process, data backup, and session control. This is a positive development, but the question is whether the healthcare staff were actually practising what they claim they knew.

In this study, security and privacy violation emerged strongly when the participants discussed their experience in relation to cyber security practice amidst their work. The violations include authentication sharing, password sharing, and unauthorised access to patients' information. When the hospitals recently adopted the EHR system, each of the healthcare staff was given legitimate access through the issuance of user credentials (a user name and passwords) for authentication and access. These credentials are usually supposed to be used by only the person to whom the credentials were given. However, it was observed that the staff were indiscriminately using sharing the user credentials with each other. For instance, a participant in the IT group of hospital A (001) shared that " I remember something happened some time ago, which i will not mention the doctor's name. A patient came to the hospital through emergency and a user credential was used on the EHR system to consult for the patient. The patient later died. However, the actual owner of the credentials was neither on duty nor on the post. So account owner was contacted regarding password sharing, and denial of having knowledge about that.

Another staff (001) in the IT group of hospital B said, he once had to share his admin credential with the accountant due to some technical issues. It later came to light that the account used the admin credentials to collect money for himself. A number of healthcare staff shared their experience to suggest that credential sharing was one of the major security issues experienced by the healthcare staff in the hospital. Regarding physical security

Authentication sharing (where a user login session is used by an unauthorised person) was also reported as a major problem. A participant of hospital A said that " sometimes when a user leaves his or her desk without logging out, unauthorised do use hat to access and view patients history without therapeutic reasons. Such actions do not only breach security measures but also breach the confidentiality of the patients involved. In exploring for the factors that are causing these violations, some of the issues were traced to moral conduct such as personal gain and peer pressure to misuse access credential. A doctor recounted how he was mopped for refusing to yield to peer pressure to misuse the EHR sytem. The participant (007) said

he was tagged as a difficult person by one of his colleague doctors as a difficult person simply because I did not allow him to use my account. The participant added that in that hospital, it is against the hospital's policy for doctors to provide healthcare to themselves. However, some doctors were circumventing that policy by exchanging their user credentials with their friends. This enables them to use their friend's accounts to provide therapeutic functions to themselves. Another participant (009) recalled a related practice among the nurses. The former said that "nurses have access to the prescription module. So during the vetting of insurance claims, we get to see drug and diagnosis miss-match. When some of the nurses are sick, instead of consulting the medical doctors, they rather prescribe the drug for themselves. We think that sometimes, they even prescribe the drug and take the medication to their friends and relative in the house.

Aside from these, work emergencies and workload were also observed to be contributing to security issues. A participant who was part of the admin or management focus group illustrated that "if a doctor wants someone to do something for the former, the former will share his credentials with the latter. Another participant (002) in the management group also agreed and said that " during an emergency, other staff tend to help the few experienced staff. So the experienced staff tend to share their user credentials with the less experience once for support. Other participants opine that usability and security design issues contribute to the security issues. For instance, a patient record can only be corrected by the use who create that record. This was shared by participant (002) from the operational staff group of hospital B. So if the person who created the record is not available, he or she would have to share their password in order to correct the error on the patient before treatment is given. Sometimes it is necessary to correct the error since the treatment of patients can be based on the records of the patients and such security restrictions encourages credentials sharing.

Regarding how participants feel about the security in the hospitals, themes relating to perceived severity, perceived vulnerability and perceived efficacy were identified. For instance, the focus-group member in the IT group of hospital B expressed that "sharing of password is my biggest fear because hackers can easily hack into the system if they get hold of these user credentials. As mentioned earlier, participants also expressed the severity of possible security breaches on patients. They feel that, downtime can tend to worsen patients' conditions and that could even lead to their death. The perceived severity of the participants is in line with a history in which a delayed treatment (caused by a ransomware attack in 2021) on a patient resulted in her death in Germany [5]. On the basis of perceived efficacy, participants have trust in the cyber security controls of the EHR as compared to the paper-based system. As recounted by a participant in hospital B in the operational staff group that "... Previously we were using folders, and

sometimes before we get to know, somebody's folder will be in court, and the doctor will be called to go to the court for the folder. The security was not tight at the time. So digitization has helped because such record stealing can not easily happen".

16.5.1 Practical implication and mitigation strategies

Following the assessment of security practices in a paperless hospital, various security measures can be taken to improve upon the security practice among the healthcare staff. From the participants' point of view, social control could serve as a deterrence measure. For instance, staff who are culpable of circumventing the system based on bad moral conduct or for self-centred purposes, need to be reprimanded to serve as a deterrence to others. This happened to be supported by Theohariduo et al, study claims that security controls of internal users could be augmented with the General deterrence theory (GDT) [32]. However, a participant from the IT group of hospital B, cautioned that GDT should be carefully introduced in order not to deter others from using the technology. In addition to the GDT, positive reinforcement should be adopted to encourage security practices. For instance, the staff who was verbally abused for failure to share his user credential could be rewarded to serve incentives for others. Training users in cyber security measures and supporting them in their use of the system were also proposed by participants to improve security practices.

Aside from these, management actions are also required in the combat against security issues in various ways. The fundamental approach to improving organizational security practices the development and adoption of an effective security policy [16]. This serves as a blueprint that specifies the security goals and objectives of the organization's needs, systems and issue specifics [37]. Since a security policy alone does not ensure compliance [8], security personnel need to be engaged to superintend and manage the entire security of the healthcare IT infrastructure by handling analysis, designs, implementations, monitoring and research, supervising, and forensic and incident handling among other related activities. The security personnel could also provide continual training and education for healthcare staff to prevent security and privacy violations such as in 18.1 and 16.2. Such activities would help to handle cyber security in a holistic way while enabling the core IT staff to efficiently handle their fundamental IT activities in their roles.

Moreover, being conscious of the healthcare needs when developing security measures, could help improve the security practice. A related study, found out that healthcare staff will circumvent security and privacy measures in order to provide healthcare if the measures obstruct the provision of therapeutic functions [19]. This can be archived by engaging healthcare staff in various roles in the development of security systems.

16.5.2 Conclusion

The human aspect of security practice in recent times has been the main driver of surges in global data breaches. As a result, an ethnographic investigation using a focus group and an observational approach was used to assess the security behaviour of the healthcare staff in two hospitals that adopted EHR systems. Having had a discussion with twenty-eight healthcare staff in six separate focus group meetings, various key themes emerged in five research guide areas. It emerged from the discussions that the healthcare staff have knowledge in security practices relating to password use, authentication sharing and other security measures, however, gross violations of security and privacy measures were experienced by the healthcare staff. These violations were majorly caused by bad moral conduct such as personal gains, peer pressure and work related factors pertaining to healthcare. Various suggestions for improving security practice have been provided including the development and implementation of the fundamental security structures such as security policies.

16.6 Bibliography

[1] ABUBAKARI, S. W., ALHASSAN, N., ADDA, R., ASANTE, K. P., AND BAWAH, A. A. Socio-economic, physical and health-related determinants of causes of death among women in the kintampo districts of ghana. *Cogent Public Health 9*, 1 (2022), 2109300. 459

[2] ALUMARAN, S., BELLA, G., AND CHEN, F. The role and impact of cultural dimensions on information systems security in saudi arabia national health service. *International Journal of Computer Applications 112*, 2 (2015). 458

[3] ANDERSON, C. L., AND AGARWAL, R. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly* (2010), 613–643. 454, 490

[4] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., AND XU, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. 272, 274, 296, 313, 404, 406, 412, 414, 442, 444, 457, 512

[5] BBC. Police launch homicide inquiry after german hospital hack, September 2020. Available from: `https://www.bbc.com/news/technology-54204356`. 467

[6] BULGURCU, B., CAVUSOGLU, H., AND BENBASAT, I. Information security policy compliance: an empirical study of rationality-based beliefs

and information security awareness. *MIS quarterly* (2010), 523–548. 454, 490

[7] GDPR. Eugdpr. key changes with the general data protection regulation â“ eugdpr, November 2022. Available from: https://eugdpr.org/the-regulation/. 454

[8] GEBRASILASE, T., AND LESSA, L. F. Information security culture in public hospitals: the case of hawassa referral hospital. *The African Journal of Information Systems 3*, 3 (2011), 1. 457, 468

[9] GEORGIADOU, A., MICHALITSI-PSARROU, A., GIOULEKAS, F., STAMATIADIS, E., TZIKAS, A., GOUNARIS, K., DOUKAS, G., NTANOS, C., LANDEIRO RIBEIRO, L., AND ASKOUNIS, D. Hospitals' cybersecurity culture during the covid-19 crisis. In *Healthcare* (2021), vol. 9, MDPI, p. 1335. 454, 490

[10] GIBBS, A. Focus groups. *Social research update 19*, 8 (1997), 1–8. 458

[11] HASSAN, N. H., MAAROP, N., ISMAIL, Z., AND ABIDIN, W. Z. Information security culture in health informatics environment: A qualitative approach. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (2017), IEEE, pp. 1–6. 457

[12] HAWORTH, J. May have snooping into the medical records of 145 patients, April 2022. Available from: https://www.nrk.no/innlandet/siktet-for-omfattende-journalsnoking-ved-sjukehuset-innlandet-1.15948310. 454

[13] HAWORTH, J. Uk government employees receive 'billions' of malicious emails per year – report, April 2022. Available from: https://portswigger.net/daily-swig/uk-governmentemployees-receive-billions&-of-malicious-emails-per-year-report. 1, 454, 490

[14] HERATH, T., AND RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems 47*, 2 (2009), 154–165. 7, 405, 412, 428, 448, 457, 493

[15] IFINEDO, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security 31*, 1 (2012), 83–95. 10, 273, 457, 496

[16] ISO. 27799:2016(en), health informatics information security management in health using iso/iec 27002. 2016., November 2016. 456, 457, 468

[17] ISO. Iso 27799:2016(en), health informatics information security management in health using iso/iec 27002, November 2016. Available from: https://www.iso.org/standard/62777.html. 454, 490

[18] JOHNSTON, A. C., WARKENTIN, M., AND SIPONEN, M. An enhanced fear appeal rhetorical framework. *MIS quarterly 39*, 1 (2015), 113–134. 454, 490

[19] KOPPEL, R., SMITH, S., BLYTHE, J., AND KOTHARI, V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise*. IOS Press, 2015, pp. 215–220. 427, 468

[20] LIN, L.-C. Data management and security in qualitative research. *Dimensions of Critical Care Nursing 28*, 3 (2009), 132–137. 455

[21] LIVERI, D., SARRI, A., AND SKOULOUDI, C. Security and resilience in ehealth infrastructures and services. *Security Challenges and Risks* (2015). 455

[22] MAYS, N., AND POPE, C. Qualitative research: observational methods in health care settings. *Bmj 311*, 6998 (1995), 182–184. 457

[23] MOFFIT, R. E., AND STEFFEN, B. Health care data breaches: A changing landscape. *Maryland Health Care Commission* (2017), 1–19. 454

[24] MOU, J., COHEN, J. F., BHATTACHERJEE, A., AND KIM, J. A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems 23*, 1 (2022), 196–236. 10, 273, 457, 496

[25] PANDA, S. Comparative analysis of qualitative and quantitative research. *M. Lib. I. Sc. Project* (2019), 1–11. 456

[26] PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., AND JERRAM, C. The development of the human aspects of information security questionnaire (hais-q). 7, 10, 278, 282, 414, 442, 443, 446, 461, 498

[27] RENAUD, K., AND GOUCHER, W. Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security* (2012). 2, 6, 454, 457

[28] RIZZONI, F., MAGALINI, S., CASAROLI, A., MARI, P., DIXON, M., AND COVENTRY, L. Phishing simulation exercise in a large hospital: A case study. *Digital Health 8* (2022), 20552076221081716. 2, 11, 14, 15, 454, 490, 492, 506

[29] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 9, 10, 12, 15, 200, 274, 405, 407, 412, 428, 446, 457

[30] SEDGWICK, P. Convenience sampling. *Bmj 347* (2013). 459

[31] SHILTON, K., SUBRAMANIAM, M., VITAK, J., AND WINTER, S. Qualitative approaches to cybersecurity research. *IConference 2016 Proceedings* (2016). 455

[32] THEOHARIDOU, M., KOKOLAKIS, S., KARYDA, M., AND KIOUNTOUZIS, E. The insider threat to information systems and the effectiveness of iso17799. *Computers & Security 24*, 6 (2005), 472–484. 468

[33] VENKATESHA, S., REDDY, K. R., AND CHANDAVARKAR, B. Social engineering attacks during the covid-19 pandemic. *SN computer science 2*, 2 (2021), 1–9. 2, 454, 490

[34] VERIZON2021. 2021 data breach investigations report, November 2021. Available from: `https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf`. 1, 270, 293, 441, 454

[35] VERIZON2021. 2022 data breach investigations report, September 2022. Available from: `https://www.verizon.com/business/resources/reports/dbir/`. 1, 454

[36] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 2, 3, 7, 23, 142, 152, 199, 200, 217, 224, 225, 236, 247, 278, 414, 442, 456, 457, 491, 498

[37] YENG, P. K., FAUZI, M. A., SUN, L., AND YANG, B. Assessing the legal aspects of information security requirements for health care in 3 countries: Scoping review and framework development. *JMIR Human Factors 9*, 2 (2022), e30050. 3, 22, 465, 468

[38] YENG, P. K., FAUZI, M. A., AND YANG, B. A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information 13*, 7 (2022), 335. 24, 455, 456, 461, 495, 501, 509

[39] YENG, P. K., SZEKERES, A., YANG, B., AND SNEKKENES, E. A. Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: Systematic mapping study. *JMIR human*

factors 8, 2 (2021), e17604. 9, 11, 15, 17, 24, 272, 273, 274, 282, 405, 406, 407, 414, 457, 496, 498

[40] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 1, 2, 6, 10, 11, 15, 17, 23, 199, 217, 224, 274, 282, 404, 405, 406, 407, 409, 410, 414, 442, 443, 454, 457, 491, 498

Part V

Motivational methods for incentivising security practice

Chapter 17

A Framework for Assessing Motivational Methods Towards Incentivizing Cybersecurity Practice in Healthcare

Prosper Kandabongee Yeng ; Bian Yang; Muhammad Ali Fauzi, Diah Priharsar

Abstract

Data breaches in healthcare have become common in recent times due to the weakness of the human element. As a result, intrinsic and extrinsic motivations were identified, analyzed, and assessed through a literature survey. After a critical gap analysis of the related studies, a framework was designed. This can be used to practically assess the effectiveness of various motivational methods for incentivizing healthcare staff toward strengthening the human aspect of security practice.

17.1 Introduction

Like any organization, addressing healthcare information security issues involve people, process, and technology [13, 12]. However, technological measures are often used to automate various security measures including patch management, antivirus update, intrusion detection and prevention, and other security policy configurations, aimed to reduce the knowledge and time burden on end-users [13]. However, overreliance on technological measures cannot succeed in addressing all the emerging threats as some are dependent on human behaviour. For instance, behaviours such as appropriate password habits, appropriate use of networks, and other conscious care behaviour are more dependent on the users [13, 31, 32].

Security issues relating to the human element have become a major concern in recent times because millions of dollars and even human lives are

being lost to security issues in healthcare. As humans are classified as the weakest link in the security chain [15, 28, 26], adversaries tend to manipulate them to complete their attack intentions in healthcare systems. Data breaches in healthcare spiked to 55% in 2020 in the US and counted up to 600 breaches with a relative increase in the cost of data breaches by 10% in comparison with that of 2019 [29]. Recently, various health providers including Ireland HSE and New Zealand hospitals went into Electronic Health Records downtime due to ransomware attacks. The HSE consists of over 100,000 workers who run the public health service in Ireland, focusing on patients and clients [14]. The root course of the attack was being investigated however, most ransomware attacks are caused by human susceptibilities. The attackers tend to lure the users to click on malicious links thereby enabling the cybercriminals to gain unauthorized access to healthcare systems.

The general objective of this study is to develop a framework that can be used to practically assess various motivational methods for improving security practices among healthcare staff. The specific objective and the contribution in this paper therefore aimed towards addressing the following research questions;

- What are the state-of-the-art motivational methods for incentivising security practices?
- How can these methods be assessed towards improving healthcare staff's security practice?

17.2 Background

In the quest for incentive methods, for reducing susceptibility in the context of human behaviour, various theories, concepts, and constructs have been imported into the space of information security research. These include Health Belief Model (HBM), Protection Motivation Theory (PMT), Cognitive dissonance (CD), General deterrence theory (GDT), Social control (SC), and many more.

PMT deals with the ability to incentivize the individual themselves based on various perceptions such as a threatening event, perceiving the probability of the occurrence, or vulnerability, perceived impact of the recommended action, and perceived self-efficacy [25]. PMT relies on fear appeals and uses self-efficacy, response efficacy, maladaptive response, and past behaviour factors. But PMT does not account for the influence of personal and demographic variables and it has been considered to have inflexible cues to action [19]. TPB/TRA adopts attitude, subjective norms, and perceived behavioural control to influence individual and organizational security culture [2, 1]. In addition, TPB accounts for social factors but it does not con-

sider psychological effects such as mood as well as environmental factors, economic effects, and prior experience. GDT discourages information security malpractices of individuals through disciplinary actions of the offenders [23]. The debate as to whether to use intrinsic or extrinsic motivations to enhance security practice requires a variety of reflections.

These theories, concepts, and constructs are usually classified into intrinsic and extrinsic motivation. Intrinsic motivation tends to induce self-motivation and it is based on self-rewarding with inherent satisfaction. This type of motivation is independent of external reward [15, 6] and provides the freedom for employees to take their own internal decisions including their aspirations [15, 27]. Extrinsic motivation is influenced by external rewards such as financial rewards or punishment towards inducing individuals to be conscious and careful of their security behaviour.

The term cognitive dissonance is used to describe the mental discomfort that results from holding two conflicting beliefs or values. For instance, knowing that sharing a password violates security practices when one is confronted with the act to share a password.

17.3 Study Approach

This study mainly assessed and developed a framework for modelling and analyzing various motivational methods for incentivizing security practices. As a result, related studies were selected in Google scholar, Pubmed, and Scopus with the search string of "Incentives OR motivation AND employee AND information security practice AND Healthcare". Literature such as peer-reviewed articles and published academic journals, relating to theoretical literature or research data-driven were included in the study.

17.4 Related studies of motivational methods for enhancing information security practice

Following the surge in data breaches, emanating from human behaviour, various research works have been conducted for motivational methods to incentivize security practices. For instance, Goel et al recently conducted research to assess the influence of financial motivation in incentivizing security practices across various organizations including healthcare staff. Participants were grouped into negative and positive frames [11]. The negative frame lost financial rewards if security policy violations were seen while participants in the positive frame were to gain financial incentives if they followed the security policy. Phishing attack with email use was adopted in this study as a security practice. Additionally, Goel et al. conducted an earlier study with smaller participants [10] where the participants gained 50 dollars per week for full compliance with the company's policies. 40 dollars

were given if one violation was detected, and if 2 violations occurred, 30 dollars was offered and followed by 20 dollars offer on the count of three violations. However, no amount was given if more than three violations were detected in a week. Phishing email and password strength were used as security practices. The researchers also provided security training. Following that, the number of participants who set weak passwords was found to be greatly reduced.

Furthermore, Chen et al assessed punishment and reward to determine better incentive security practices. Three factors such as punishment, financial reward, and certainty of control were considered and these factors were administered to the participants at two levels thus severe and mild punishment, high and low reward, and high and low certainty. Security practices on password use, e-mail use, and Internet use were initially used. Oral praising was given to those who followed these policies while those who deviated, were orally reprimanded and had some points reduced per the severity of the violations. These merit points were linked to their annual bonus which was added to their salary. General Deterrence Theory (GDT) combined with financial reward was hence used in this study [7]. Other extrinsic motivational methods which were assessed include penalties and pressures [13]. However, the severity of the penalty was assessed to have a negative effect on security compliance. The finding was realized in a questionnaire survey relating to pressures exerted by subjective norms, peer behaviours influence, motivation of employees perceived effectiveness of their actions, penalties with a certainty of detection, and severity of punishment in relation to IS violations.

Besides, protection motivation theory (PMT) [21, 30] is one of the intrinsic methods which has been widely assessed to incentivize human behaviour. In the context of information security compliance, Posey et al used PMT to survey the impact of organizational motivation on individual behaviour. The study realized that the influence of PMT is much reliant on the employee's organizational commitment level. Similarly, PMT and habit were used to assess the influence of past behaviours concerning security practices. The survey employed sharing passwords, workstation locking, and logging behaviour, allowing reading of confidential material, unauthorized installations and, copying sensitive information to a USB stick without encryption, were assessed. Perceived severity (PS) was claimed to have a positive influence on security practice [21]. However, John et al claimed that cognitive effect (thus individual feeling state or how one feels at a point in time) such as the individual mood has a significant impact on security behaviour which is independent of their past habits. In this study, the theory of recent action (TRA) and the theory of planned behaviour (TPB) were used with daily information security compliance [9].

Moreover, Safa et al conducted a study and found out that increasing the

effort, increasing the risk, and removing excuses and rewards towards information security misbehaviour improves information security practice [24]. Their study was conducted by observing security practices that have increased the difficulty of violating information security policy such as strengthening access control, preventing unauthorized data exfiltration, and strong enforcement of passwords, among others. A similar issue emerged when Renaud et al had an intensive interview with the national health service (NHS) workers in the UK to find out what motivates or demotivates them in terms of information security practice in healthcare [22]. What came to light was that operational requirements for security conflicted with intrinsic motivational needs for staff, thereby causing stress and non-compliance. Staff reported helplessness when they encountered information security operational difficulties. Staff also felt subdued to following security requirements, and that following security policy was challenging, citing concerns for patients and their desire to work efficiently and effectively. In addition, studies by Lebek et al. opined that the motivation for security practice also depends on the leadership style [15]. Therefore, they conducted research into the transformational type of leadership. Transformational leaders believe in societal values and influence their followers as such. A survey was therefore conducted by using transformational leadership attributes from the multifactor leadership questionnaire to assess the security policy compliance of staff. The findings showed a positive correlation between security practice and transformational leadership.

Additionally, cognitive dissonance theory was also assessed in a related study [20] for mitigating insider threat neutralization. A Honey port and a honey token were used to bait insiders to attack the honey port in this experiment, rather than attacking real data. Factors such as the removal of excuses were used to decrease rationalizations. In the same vein, Barlow et al., analyzed denial of injury, the metaphor of the ledger, and the defence of necessity aspects of rationalization for non-compliance with password security measures [4]. The findings showed that focusing on neutralization techniques is as effective as those of deterrence sanctions.

In the exploration of effective incentive methods, Ng et al also investigated into computer behaviour of users, using the health belief model (HBM) [18]. Their study found perceived susceptibility, benefits, and self-efficacy to be determinants of email-related security behaviour. Anwar et al. also showed that gender has an effect on security self-efficacy [3]. In summary, the motivational theories and concepts which were identified are shown in Table17.1.

Table 17.1: Motivational Concepts or Theories

No	Concept/Theories	Category	Count #
1	Financial Inventive [11, 10, 7]	Extrinsic	3
2	GDT [7]	Extrinsic	1
3	PMT [21, 30]	Intrinsic	2
4	Habit	Intrinsic	1
5	Perception of IS governance [22]	Intrinsic	1
6	Theory of Planned Behavior (TPB) or theory of recent action (TRA) [9]	Extrinsic	1
7	Individual mood [9]	Intrinsic	1
8	Penalties [13]	Extrinsic	1
9	Pressures [13]	Extrinsic	1
10	Perceived effect of user's action [13]	Intrinsic	1
11	Transformational leadership [15]	Intrinsic	1
12	The increasing complexity of security behaviour [24]	Extrinsic	1
13	HBM [18, 3]	Intrinsic	2
14	CD [20, 4]	Intrinsic	2

17.5 Motivational methods, gap analysis and discussion

In efforts to strengthen human efforts in security requirement compliance, various motivational methods for incentivizing security practices were explored. The identified theories include but are not limited to HBM, PMT/TRA, CD, and GDT as shown in Table 17.1. The related theories and constructs were classified into intrinsic and extrinsic incentives. The intrinsic motivations include PMT, Perception of IS governance [22], individual mood, habits, the perceived intention of users' behaviour, and cognitive dissonance.

TPB, GDT, pressure, the increasing complexity of security behaviour [24] and financial rewards are some of the extrinsic motivations. Extrinsic motivations include the use of resources such as financial rewards. While considering the adoption of extrinsic motivation, it is vital to recognize that the healthcare environment is characterized by varying stresses that is usually originated from workload and work emergencies. For instance, during an emergency, the healthcare provider is time-bound. Therefore, incentive measures need to be carefully assessed while taking into consideration, the healthcare work-related factors. Reflecting on Goel et al study "Understanding the role of incentives in security behaviour", the study [11, 10] provided preliminary knowledge on financial incentives to enhance security however, the introduction of financial incentives for security compliance can raise the financial burden of the healthcare facility. Already, the healthcare sector has been observed to be chronically underfunded, and that has created huge burdens such as understaffing, inadequate patient care, and lack of medical equipment and consumables. As a result, the financial incentive, even if effective, may not be sustainable. Besides, bearing in mind that resources are limited, especially in organizations with many users, the adoption of financial motivation can have a huge burden on the organization such that if financial promises are not paid for for good security practices, the staff me

tend to misbehave. Moreover, when thinking about assessing, punishment in GDT as an extrinsic measure, there is the need to be aware that maladaptive behaviour can set in such that the healthcare staff can also tend to not follow security practices. Healthcare staff may also feel subjugated by authorities to comply with security practices. Aside, punishment may be the last option for an organization to strictly adopt to induce sound security practices. The reason is that healthcare staff can be faced with stress from patients' conditions, emergency cases, and high workloads that can be contributing factors affecting security practice. Therefore, healthcare workers may feel unappreciated if they are punished due to unintentional security violations.

In the case of intrinsic motivations, studies have pinpointed leadership style and the lack of consideration of healthcare operational requirements to have a negative correlation with conscious care security practice [15, 22]. For example, Renaud et al found that security policy requirements interfered with the staff' intrinsic motivational needs, which led to their stress and non-compliance. Due to the leadership style, staff often felt suppressed with policies, with no support. Additionally, the motivations of IT security officers to ensure security was often in conflict with that of the operational staff who were more concerned about their patients and the need to complete their tasks.

To this end, various studies called for the adoption of both intrinsic and extrinsic motivation in the incentivization scheme for conscious care behaviour [15, 22] Safa et al., also advised management to consider the environmental factors that encourage employees to engage in information security misbehaviour and dealing with these environmental factors by putting in appropriate measures to decrease their negative effects on employees' security behaviour to mitigate the risk of insider threats. Virtual reality (VR) technology can also be assessed in this context [16, 17] where for instance, intrinsic factors are simulated with these devices to induce other psychological effects on healthcare staff such as fear appeals, perceived severity, perceived vulnerability, and low-risk rationalization of cognitive dissonance. The framework in Figure **??** can be followed to assess and incorporate both intrinsic and extrinsic incentives toward enhancing security practice.

From the existing studies, a control experiment method [7, 11] and field observations [18, 3, 20, 4, 24, 15] were the identified methods often used to assess the effect of motivation factors to incentivize security practice. With regards to a control experiment, the participants are usually assigned into groups followed by administering a treatment or an intervention to one of the groups, while the other groups (controlled group) are not provided with any intervention [8]. Even if an intervention is provided in the controlled group, that intervention is varied across the groups. In that the observational study, participants are surveyed with the aim to observe some fac-

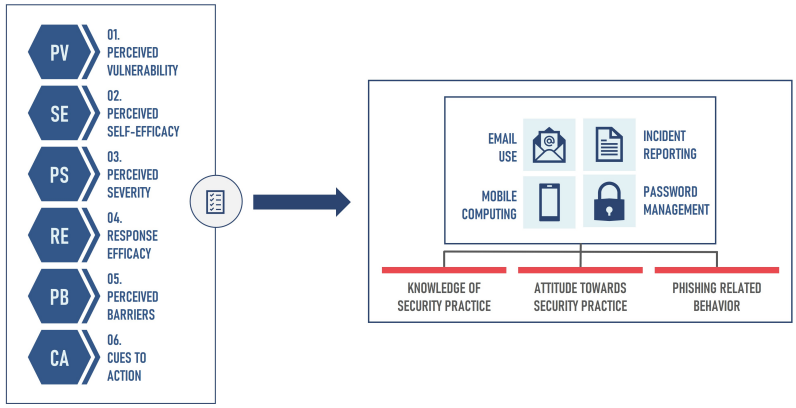


Figure 17.1: A framework for assessing motivational methods toward incentivizing security practice.

tors without varying interventions among the participants. The controlled experiment has been considered to be useful in determining the cause-and-effect relationship between variables [5]. Hence, we adopted a control experiment in determining the influence of motivational factors on incentivising security practice.

17.6 A Control experiment framework for assessing motivations in security practice

The healthcare staff, including the doctors and nurses, are usually required to follow security practices including password management, incident reporting, and email use as shown in Figure 17.1. Additionally, the knowledge, attitude, and behaviour (KAB) of users with these security practices in TPB are usually essential in their actual security practice. The security practices combined with the KAB of the healthcare staff can be related to the various constructs such as PV, PS, SE, and RE to form a study scope.

A control experiment can then be conducted to assess the effectiveness of these constructs. For instance, the control experiment could have two levels, thus, a control group and an experiment group. The experiment group will then be treated with various theories, constructs, or concepts such as cognitive dissonance. The effect of the treatment can then be measured with the study scope. The assessment can be done with survey instruments, practical assessment with attack and defence simulation or directly observing the two groups to determine the effect of the treatment on the security practice of the

participants. The treatment can be done by exposing participants in the experiment group to the independent variable through training, gamification, and the use of virtual augmented or mixed reality.

17.7 Conclusion

In search of ways to enhance security practices in healthcare, a survey was conducted to identify and assess various motivational methods. Extrinsic motivational methods such as financial incentives and deterrence methods were found. Also, other intrinsic methods were identified to include fear appeals from protection motivation theory, cognitive dissonance, leadership style, and preventing conflict between healthcare operational goals and required security practice of healthcare staff. To this end, a framework was proposed for assessing the efficacy of the various motivational constructs for enhancing healthcare security practice.

17.8 Bibliography

[1] AJZEN, I. The theory of planned behavior. *Organizational behavior and human decision processes 50*, 2 (1991), 179–211. 478

[2] AJZEN, I., AND MADDEN, T. J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology 22*, 5 (1986), 453–474. 478

[3] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., AND XU, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69* (2017), 437–443. 481, 482, 483

[4] BARLOW, J. B., WARKENTIN, M., ORMOND, D., AND DENNIS, A. Don't even think about it! the effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems 19*, 8 (2018), 3. 481, 482, 483

[5] BENZEL, T. The science of cyber security experimentation: the deter project. In *Proceedings of the 27th Annual Computer Security Applications Conference* (2011), pp. 137–148. 484

[6] BROWN, L. V. *Psychology of motivation*. Nova Publishers, 2007. 479

[7] CHEN, Y., RAMAMURTHY, K., AND WEN, K.-W. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems 29*, 3 (2012), 157–188. 480, 482, 483

[8] COOLICAN, H. *Research methods and statistics in psychology*. 2017. 18, 20, 483

[9] D'ARCY, J., AND LOWRY, P. B. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal 29*, 1 (2019), 43–69. 480, 482

[10] GOEL, S., WILLIAMS, K., HUANG, J., AND WARKENTIN, M. Understanding the role of incentives in security behavior. 479, 482

[11] GOEL, S., WILLIAMS, K. J., HUANG, J., AND WARKENTIN, M. Can financial incentives help with the struggle for security policy compliance? *Information & Management 58*, 4 (2021), 103447. 479, 482, 483

[12] HAMILL, J. T., DECKRO, R. F., AND KLOEBER JR, J. M. Evaluating information assurance strategies. *Decision Support Systems 39*, 3 (2005), 463–484. 477

[13] HERATH, T., AND RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems 47*, 2 (2009), 154–165. 477, 480, 482

[14] HSE. Hse code of governance, 2021. Available from: `https://www.hse.ie/eng/about/who/directoratemembers/codeofgovernance/governance.html`. 478

[15] LEBEK, B., GUHR, N., AND BREITNER, M. Transformational leadership and employees' information security performance: the mediating role of motivation and climate. 478, 479, 481, 482, 483

[16] MAKRANSKY, G., BORRE-GUDE, S., AND MAYER, R. E. Motivational and cognitive benefits of training in immersive virtual reality based on multiple assessments. *Journal of Computer Assisted Learning 35*, 6 (2019), 691–707. 483

[17] MAKRANSKY, G., TERKILDSEN, T. S., AND MAYER, R. E. Adding immersive virtual reality to a science lab simulation causes more presence but less learning. *Learning and instruction 60* (2019), 225–236. 483

[18] NG, B.-Y., KANKANHALLI, A., AND XU, Y. C. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 4 (2009), 815–825. 481, 482, 483

[19] NORMAN, P., AND CONNER, P. Predicting health behaviour: a social cognition approach. *Predicting health behaviour 1* (2005). 478

[20] PADAYACHEE, K. An insider threat neutralisation mitigation model predicated on cognitive dissonance (itnmcd). *South African Computer Journal 56*, 1 (2015), 50–79. 481, 482, 483

[21] POSEY, C., ROBERTS, T. L., AND LOWRY, P. B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems 32*, 4 (2015), 179–214. 480, 482

[22] RENAUD, K., AND GOUCHER, W. Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security* (2012). 481, 482, 483

[23] ROSS, E. A. Social control. *American Journal of Sociology 1*, 5 (1896), 513–535. 479

[24] SAFA, N. S., MAPLE, C., WATSON, T., AND VON SOLMS, R. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of information security and applications 40* (2018), 247–257. 481, 482, 483

[25] SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., AND HERAWAN, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78. 478

[26] SIPONEN, M., PAHNILA, S., AND MAHMOOD, A. M. A new model for understanding users' is security compliance. 478

[27] SIPONEN, M. T. A conceptual foundation for organizational information security awareness. *Information management & computer security* (2000). 479

[28] SPEARS, J. L., AND BARKI, H. User participation in information systems security risk management. *MIS quarterly* (2010), 503–522. 478

[29] VAIDYA, A. Report: Healthcare data breaches spiked 55% in 2020, Feb. 2021. Available from: `https://medcitynews.com/2021/02/report-healthcare-data-breaches-spiked-55-in-2020/#:~:text=There%20were%20nearly%20600%20healthcare,breach%20increased%20by%20about%2010%25`. 478

[30] VANCE, A., SIPONEN, M., AND PAHNILA, S. Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management 49*, 3-4 (2012), 190–198. 480, 482

[31] YENG, P., YANG, B., AND SNEKKENES, E. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (2019), vol. 2, IEEE, pp. 397–404. 477

[32] YENG, P. K., YANG, B., AND SNEKKENES, E. A. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245. 477

Chapter 18

Exploring cognitive dissonance towards mitigating phishing susceptibility in healthcare: A controlled experiment based on phishing sim- ulation attack in an actual hospital

Prosper K. Yeng, Muhammad A. Fauzi, Bian Yang, Arnstein Vestad, Katrien R.D. Moor and Christian Jacobson

This paper is awaiting publication and is not included

ISBN 978-82-326-7044-4 (printed ver.)
ISBN 978-82-326-7043-7 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

NTNU
Norwegian University of
Science and Technology