Healthcare Staffs' Information Security Practices Towards Mitigating Data Breaches:Literature Survey

Prosper Kandabongee Yeng, Bian Yang and Einar Arthur Snekkenes
Department of Information Security and Communication Technology
Norwegian University of Science and Technology, Gjøvik, Norway

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 emperical studies in a hospital setting in Norway on Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI). Human Aspect of Information Security Questionnaire was identified as robust and comprehensive tool for gathering staff security practices. Integrated theories was being adopted to form a comprehensive staffs' characteristics. A mixed-method for evaluating the theories was also identified to be the best strategy.

Keywords. Social-Culture, Information Security, Social Demography, Healthcare Staff

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[1]. 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[2]. Healthcare data is richer than data in the financial sector[3] and it costs ten times more than credit cards data from banks in the underground cyber markets[3]. 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[4]. Stolen healthcare data can also be used to obtain medical treatment and gaining access to credit card information[4].

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 [5]. 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 [1] and the consequences ranges from fraud to loss of human lives [6] and fines up to Twenty Million Euros[7]. The annual

estimated losses from cybercrime is forecasted to reach USD 2 trillion from few years to come[8]. Though security in healthcare extend beyond ICT related systems [8], 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[9]. 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[10]. Socio-demographic characteristics in this study include age, gender, education, workload level, emergency situation and the security experience while psycho-socio-cultural characteristics in this study, is referred to personal behaviors that are influenced by psychological, social and cultural factors including perception, attitude, norms and beliefs[11]. Other healthcare staffs' 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) [12]. 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[13]. Healthcare staffs are required to be confidential with patients information[14], 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 employee have been adopted in this study to be synonymous and were used interchangeably. The healthcare staffs 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 belief, healthcare emergency situations, workload, security perceptions, age, gender and experience 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 practices of healthcare staffs which often have a significant impact on security.

2. Method

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 in behavioral 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-arts relating to modeling staffs' characteristics, staffs' security practices and evaluation techniques.

3. Results

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[14]. The significance of these traits could undermine IS policies and regulations which can lead to IS violations[14]. 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[12]. 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.[12] 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 considered in the combined framework[15]. Furthermore, a Health Belief Model (HBM)[16] 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 the 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)[17]. 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 [18], personality traits are stable over time and it 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[11] [17]. Anwa et al.[11] 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 ($r=-.152$, $p< .001$) [11]. Roer et al.,, conducted a security culture study in Norway and Sweden among 10,000 employees across different industries[19]. 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.

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[15] [16]. 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[20]. 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[12] [11] [14] [16]. Other studies including relied on Authentication, De-Authentication and Permission Management. However, these security practices alone do not constitute a holistic policy requirement[20] 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[18]. HAIS-Q security practices includes internet use, email use, social media use, password management, incident reporting, information handling and mobile computing[18]. But the tool is required to always be updated to reflect current IS standards and policies prior to usage[18].

3.3. State-of-the-art-studies relating to Evaluation Techniques

On the part of the evaluation of these theories, most of the studies, [12] [11] [14] [16], used survey with only questionnaire instrument in a quantitative study. A study which was conducted in a healthcare setting [21], used only interview and observational method in a qualitative study. Rezgui, et al., employed interview, questionnaires and observation [22] in a mixed method. The main merit of quantitative method approaches to qualitative analysis is that the findings can be implemented to 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[22].

In summary, the various theories were categories into some aspect of HSPAMI study areas as shown in Table 1.

Table 1: Analysis of the theories and their application areas in HSPAMI

HSPAMI study area	**Theories that support study area**
Social Bonding (SB)	SC[12]
Peer Pressure (PP)	SC[12]
Social Norms and Beliefs (SNB)	SC, HBM[12, 16]
Healthcare Emergency (HCE)	PMT, SC, TPB[9, 12, 23]
Work Load (WKL)	PMT, HBM[16, 23]
Privacy and Security perception	PMT, DT, HBM[12, 16, 23]
Personality and Attitude (PA)	TBF, TPB, HBM[9, 16, 18]
IS Experience, Education and Knowledge (IEEK)	PMT[16]
Emotions	PMT, HBM [9, 16]

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"[16, 24]. 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 [14]. PMT deals with the ability to protect oneself base on; perceived severity of a threatened event, perceived probability of the occurrence, or vulnerability, the impact of the recommended preventive behavior and perceived self-efficacy[9]. PMT primarily uses the influence of fear appeals and considers factors such as self-efficacy, response efficacy, maladaptive response and past behavior. However, PMT has 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[25]. TPB is the use of attitude, subjective norms, and perceived behavioral control to influence individual way of life[26, 27].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[9] 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[12, 15]. GDT mission is to discourage misbehaviors of other persons through disciplinary measures of the offenders but does not consider social, economic or environmental factors[23]. GDT is deemed not effective and has not been considered in this study[12].

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[28]. 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, [9, 12, 29] 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[20]. But HAIS-Q tool was explored in a study

involiving conscientiousness, agreeableness, emotional stability and risk-taking tendency[18]. 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[18]. HAIS-Q can be used to model the variables in HSPAMI and it can be updated to meet the healthcare study need[20]. 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 [18, 20].

Some studies [11, 12, 19, 29] 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[22]. 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[30]. Different sources of data for decision making is also in line with the idea of combining multiple perceptions to draw a valid conclusion[31]. The main disadvantage of multiple data collection is cost[22] since observation may require more time[31].

5. Conclusion and Future Works

This literature survey was conducted to explore for theories and evaluation strategies being used to efficiently study into 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 into 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 a holistic healthcare staff security practices for studies into HSPAMI. An integration approach of theories such as HBM, SC, TBF, PMT, TPB would be combined to obtain the needed healthcare staffs' 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 questionnaire, 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.

6. References

[1] Manadhata, P.K. and J.M. Wing, An Attack Surface Metric. IEEE Transactions on Software Engineering, 2011. 37(3): p. 371-386.

[2] @digitalhealth2. Norway healthcare cyber-attack could be biggest of its kind. 2018 2018-01-24 [cited 2019 01-02-2019]; Available from: https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/.
[3] C. Humer and J. Finkle, Your medical record is worth more to hackers than your credit card, in Reuters. 2014, Reuters.com 24: US.
[4] Lawrence Pfleeger, S., et al., Insiders Behaving Badly: Addressing Bad Actors and Their Actions. IEEE Transactions on Information Forensics and Security, 2010. 5: p. 169-179.
[5] Tetz, E. Network Firewalls: Perimeter Defense - dummies. 2018 [cited 2019 03.03.2019]; Available from: https://www.dummies.com/programming/networking/cisco/network-firewalls-perimeter-defense/.
[6] Robert E. Moffit and B. Steffen, Health Care Data Breaches: A Changing Landscap. 2017.
[7] EUGDPR. Key Changes with the General Data Protection Regulation â□“ EUGDPR. 2019; Available from: https://eugdpr.org/the-regulation/.
[8] ISO, ISO 27799:2016(en), Health informatics â€ ” Information security management in health using ISO/IEC 27002. 2016.
[9] Safa, N.S., et al., Information security conscious care behaviour formation in organizations. Computers & Security, 2015. 53: p. 65-78.
[10] Yuryna Connolly, L., et al., Organisational culture, procedural countermeasures, and employee security behaviour. Information and Computer Security, 2017. 25(2): p. 118-136.
[11] Anwar, M., et al., Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 2017. 69(C): p. 437-443.
[12] Cheng, L., et al., Understanding the violation of IS security policy in organizations. Computers and Security, 2013. 39: p. 447-459.
[13] GESIS - Leibniz Institute for the Social Sciences. Socio-demographic characteristics. 2019; Available from: https://www.gesis.org/en/gesis-survey-guidelines/instruments/survey-instruments/socio-demographic-variables/.
[14] Debra Box, D.P., Improving Information Security Behaviour in the Healthcare Context. Social and Behavioral Science, 2013. 9: p. 1093-1103.
[15] Ross, E.A., Social Control Edward Ross 1896. American Juurnal of Sociology, 1896. 1: p. 513-535.
[16] Ng, B.-Y., A. Kankanhalli, and Y.C. Xu, Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 2009. 46(4): p. 815-825.
[17] McCormac, A., et al., Individual differences and Information Security Awareness. Computers in Human Behavior, 2017. 69: p. 151-156.
[18] Shropshire, J., et al. Personality and IT security: An application of the five-factor model. in AMCIS 2006 Proceedings. 415. 2006.
[19] Kai Roer, G.P., Indepth insights into the human factor-The 2017 Security Culture Report. 2017.
[20] Parsons, K., et al., The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 2017. 66: p. 40-51.
[21] Koppel, R., et al., Workarounds to computer access in healthcare organizations: you want my password or a dead patient? Stud Health Technol Inform, 2015. 208: p. 215-20.
[22] Rezgui, Y. and A. Marks, Information security awareness in higher education: An exploratory study. Computers & Security, 2008. 27(7-8): p. 241-253.
[23] Lebek, B., et al. Employees' Information Security Awareness and Behavior: A Literature Review. in 2013 46th Hawaii International Conference on System Sciences. 2013.
[24] Jeffrey M Stanton, K.R.S., Paul Mastrangelo,Jeffrey Jolton, Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. Compter and Security, 2004. 24(2): p. 124-133.
[25] Conner, M. and P. Norman, Predicting health behaviour: Research and practice with social cognition models. Vol. 24. 2005. 402.
[26] Ajzen, I., Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. Journal of Applied Social Psychology, 2002. 32(4): p. 665-683.
[27] Ajzen, I. and T.J. Madden, Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. Journal of Experimental Social Psychology, 1986. 22(5): p. 453-474.
[28] Davis, F.D., Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 1989. 13(3): p. 319-340.
[29] Fernandez-Aleman, J.L., et al., Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int J Med Inform, 2015. 84(6): p. 454-67.
[30] Bonoma, T.V., Case Research in Marketing Opportunities, Problems, and a Process. Journal of Marketing Research, 22, 199-208. - References - Scientific Research Publishing. 1985.
[31] Stake, R.E., The art of case study research. The art of case study research. 1995, Thousand Oaks, CA, US: Sage Publications, Inc. xv, 175-xv, 175.