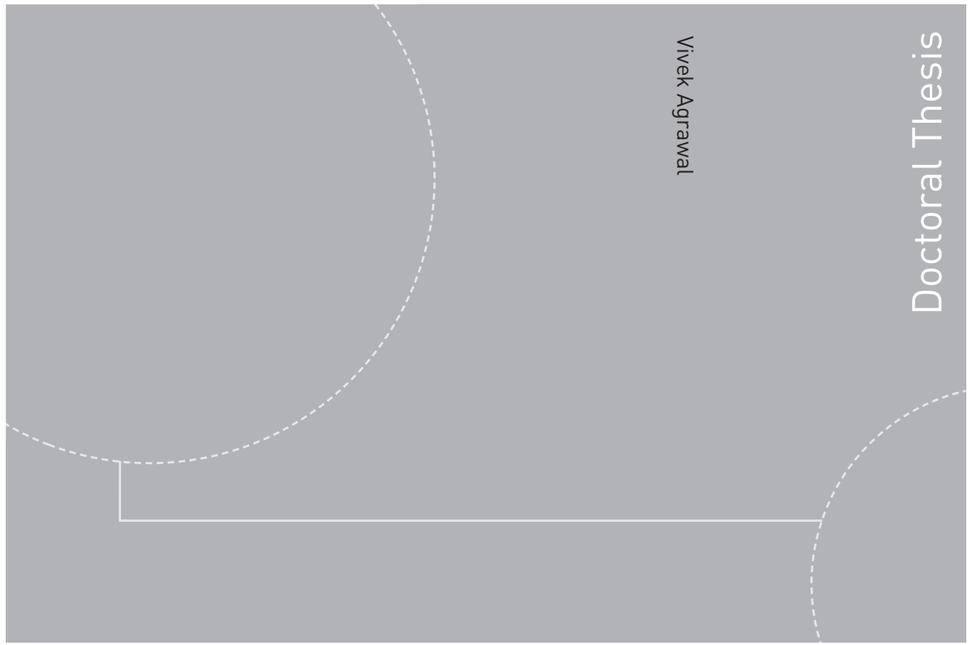
ISBN 978-82-326-3356-2 (printed version)
ISBN 978-82-326-3357-9 (electronic version)
ISSN 1503-8181



Doctoral theses at NTNU, 2018:283

Vivek Agrawal

Information Security Risk Management Practices

Community-Based Knowledge Sharing

Doctoral theses at NTNU, 2018:283

NTNU
Norwegian University of Science and Technology

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

NTNU
Norwegian University of Science and Technology

Vivek Agrawal

Information Security Risk Management Practices

Community-Based Knowledge Sharing

Thesis for the degree of Philosophiae Doctor

Gjøvik, October 2018

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

ISBN 978-82-326-3356-2 (printed version)
ISBN 978-82-326-3357-9 (electronic version)
ISSN 1503-8181

Doctoral theses at NTNU, 2018:283

Printed by Skipnes Kommunikasjon as

Dedicated to the memory of my father, Upendra Kumar Agrawal, who always believed in my ability to be successful in the academic arena. You are gone but your belief in me has made this journey possible.

Declaration of Authorship

I, Vivek Agrawal, 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:

(Vivek Agrawal)

Date:

Abstract

Information security risk management (ISRM) is an integral part of the management practice and is an essential element of good corporate governance. ISRM helps to identify and manage potential problems that could undermine key business initiatives or projects. There are several challenges associated with conducting ISRM tasks successfully in an organization. Knowledge sharing is an essential part of an organization in exploiting benefits concerning performance, decision making, and transparency. Thus, it is also important to share knowledge related to ISRM practices. Sharing and reuse of knowledge can improve both quality and the process cost-effectiveness of ISRM. A decision-maker can make a valid decision and reduce risks in an organization by receiving the right information at the right time from different sources. Organizations can be in a better position to counter attacks or risk by sharing knowledge related to attackers and methods of attacks.

The thesis aims to enhance knowledge sharing practice to solve the challenges faced by the Information Security Practitioners (ISPs) through the establishment of a working electronic community of practice (eCoP), UnRizkNow. Online questionnaires were designed to understand the factors that affect their participation and willingness to share knowledge on eCoP. ISPs affiliated with Information Security Forum (ISF) and ISACA - Norway chapter were involved in the process of data collection. The responses collected from the ISPs give an insight into their present level of participation in eCoP and the details of various factors that influence them to share or hoard their knowledge on eCoP. The study shows that the members of eCoP are reluctant to participate actively and share knowledge with other community members. Members often fear that they possess valuable and sensitive knowledge in the community and it may ruin their reputation or normal functioning if the other members misuse the knowledge. Several theories were studied to understand the knowledge sharing behavior of an individual and in a

community-based knowledge sharing settings. The research revealed that the findings of the initial research comply with the well-known theories such as the social exchange theory, the theory of planned behavior, the social presence theory, and the perceived trust theory.

This thesis also explores the theoretical and practical issues in establishing UnRizkNow community for the ISPs. The thesis employs the Design Science Research Method (DSRM) in applying the existing theories and models from the domain of information sharing, information security, behavioral science, and risk management to understand the significant factors that are necessary to establish a working eCoP and encourage the sharing of the knowledge among ISPs. A novel approach of assessing the risk in establishing and maintaining UnRizkNow community was evaluated based on the idea of human factors. Hence, the CIRA method was employed to assess the human-related risks the community may face because of the conflicts in the interests of the involved stakeholders. This study showed how the various incentives of the members and the organizer of UnRizkNow community might conflict with each other and create potential risk in the community. Furthermore, a treatment plan was developed based on the guideline of the CIRA method to mitigate the identified risk.

Moreover, the study aims to understand the ISPs perspective concerning the preferred knowledge sharing features on an eCoP. A quantitative approach was employed to carry out the research, and an online questionnaire is created to communicate with the ISPs in Norway. A knowledge sharing model based on the *purpose*, *motivation*, *preference*, and *the facilitating condition* was developed for UnRizkNow community. Furthermore, an online questionnaire was designed to cover the questions related to the elements and sub-elements of the knowledge sharing model. The participants of the online questionnaire were the ISPs working as a full-time in Norway. The data collection activity revealed various factors that are imperative in establishing UnRizkNow community platform. The features of the UnRizkNow were designed such that the information accessible in the platform will help the members to search the information easily and quickly, get up-to-date information quickly, get more relevant content, establish reputation in the community, identify the members/ post that is trustworthy, and get information in a more collected way.

The survey shows that the ISPs were willing to share their knowledge with the members of the electronic community. However, ISPs fear that the community members may misuse the sensitive information shared on the community. The communities that fail to provide a secure way of sharing the knowledge of the member also fail to improve knowledge sharing practices. The study identifies that the present benchmarking system in the information security domain faces

several security-related challenges. The benchmarking system does not ensure the confidentiality of the shared information and security during the calculation of benchmarking results. Therefore, a novel approach of encouraging participation on benchmarking task and sharing of knowledge on UnRizkNow platform is proposed in this thesis. A secure benchmarking system was proposed using the electronic voting approach. The concepts of the benchmarking system is mapped to the concepts of the electronic voting system. The secure benchmark system inherits the security properties from the electronic voting system and ensures the confidentiality of the shared information, and the identity of the members. The proposed solution will be helpful to engage UnRizkNow members in sharing sensitive knowledge through the secure benchmarking system.

Acknowledgments

This research was carried out during the years 2014-2018 at the Department of Information Security and Communication Technology (IIK), Norwegian University of Science and Technology (NTNU Gjøvik). The research work, reported in this thesis, is a part of the UnRizkNow project funded by the Center for Cyber and Information Security (CCIS) and NTNU.

I owe my most profound gratitude to my principal supervisor Prof. Dr. Einar Arthur Snekkenes. This study would hardly have been completed without his continuous guidance, enthusiasm, encouragement, and support. His advice and support have been invaluable on both an academic and personal level, for which I am incredibly grateful. I also express my warmest gratitude to my co-supervisor Prof. Dr. Stewart James Kowalski, who helped me in understanding many concepts of Information Security Risk Management. In addition, I would like to thank the evaluation committee members, Prof. Dr. Louise Yngström, Prof. Dr. Alexandre Ardichvili, and Assoc. Prof. Dr. Bian Yang, who agreed to review the thesis and provide the valuable comments.

I am indebted to my co-authors who helped to achieve my research objectives by sharing their skills, expertize, and valuable time. I want to thank Pankaj Wasnik for helping me with the statistics, Adam Szekeres for helping me investigate the human-based risk using CIRA method, and Dr. Thomas Kemmerich for helping me understand the cloud computing area. I want to thank my colleagues Gaute Wangen, Martin Stokkenes, Shao-Fang Wen (Steven), Pankaj Pandey, Vasileios Gkioulos, Andrii Shalaginov, Roberto Rigolin Ferreira Lopes, Romina Muka, Ambika Chitrakar, Edlira Martiri, and others. I had a fantastic experience spending time in your company.

I would like to acknowledge the financial support provided by NTNU, CCIS, and

COINS; academic support by NTNU and UIO, administrative support by Nils Karlstad Svendsen, Kathrine Huke Markengbakken, Urszula Nowostawska, Rachael McCallum, Hilde Bakke, Jingjing Yang, Stein Runar Olsen, and Ingrid Schantz Bakka; technical support by the IT department of NTNU, and notably Lars Erik Pedersen for helping me conduct performance testing, and server configuration of UnRizkNow platform.

I want to show my gratitude to NorSIS, ISF Norway, and ISACA Norway who helped me in my research work by participating in the online questionnaire and allowing me to conduct a data-collection workshop with the Information Security Practitioners in Norway. I want to thank all the members who participated in my online survey. Your response helped me to materialize my research findings.

Most importantly, I would like to thank my wife, Jiggyasa Agrawal, for her continuous encouragement and support throughout my studies. I am also grateful to my mother and all my family members for their support and love.

Contents

List of Tables

List of Figures

List of Abbreviations and Definitions

Abbreviations

A Election Administrator

ACP Admin Control Panel

ASE Academic Staff Efficacy

AUC Area Under ROC Curve (AUC)

BA Benchmark Administrator

BCA Benchmark Calculating Agent

BS Benchmark Submitters

CA Certification Authority

CIA Confidentiality, Integrity, and Availability

CIRA Conflicting Incentives Risk Analysis

CoP Community of Practice

CSRM Cyber Security Risk Management

DSRM Design Science Research Methodology

eCoP Electronic Community of Practice

EV Electronic Voting

InfoSec Information Security/ Information Security Risk Management

IS Information Security

ISACA Information Systems Audit and Control Association

ISF Information Security Forum

ISO27005 ISO/IEC 27005:2011 Information technology, Security techniques, Information security risk management

ISPs Information Security Practitioners/Professionals

ISRM Information Security Risk Management

IST Information Society Technologies

IT Information Technology

KSB Knowledge Sharing Behaviors

OWL Web Ontology Language

PoS Part of speech

PTT Perceived Trust Theory

RA Risk Analysis

RDF Resource Description Framework

RM Risk Management

ROC Receiver Operating Curve

RQ Research Question

SDT Self-Determination Theory

SET Social Exchange Theory

SoC Sense of Community

SPT Social Presence Theory

SSL Secure Socket Layer

TMB Theory of Motivation and Barriers

TPB Theory of Planned Behavior

UML Unified Modeling Language

Definitions

ISPs Information security practitioners/professionals: A person possesses the expertise in Application security, Network defense, Intrusion detection Digital forensics and incident response, Endpoint protection, Governance, risk and compliance

ISRM Information Security Risk management is the set of systematic activities used to direct and control an organization with regard to risk

Part I

Overview

Chapter 1

Introduction

This chapter provides an introduction to the research work. The first section provides an overview of the UnRizkNow project concerning the project objective, the project architecture, and phases in the project. The second section presents the motivation and problem description. The third section describes the research objectives, research questions, and the research design along with the details of the research flow and the associated research publications. Further, an overview of the research publications, scope, and outline are presented in this chapter.

1.1 An overview of the UnRizkNow project

The study in the thesis is based on the research work carried out in the UnRizkNow project at the Norwegian University of Science and Technology (NTNU). The project was partially funded by the Center for Cyber and Information Security (CCIS), and the duration of the project was from January 2016 to December 2017.

Project objective: There are several ad-hoc groups available on LinkedIn, Facebook dedicated to information security (IS) and information security risk management (ISRM) related topics. However, the existing groups lack the active members who share relevant knowledge. Moreover, the knowledge available in these groups are not updated regularly, or the topic of the knowledge is irrelevant to most of the members. Thus, an open electronic community of practice can be a useful tool in enabling collaboration among the ISPs and enabling the sharing of essential ISRM knowledge among them. The objective of the UnRizkNow project is to establish an electronic community of practice (eCoP) for the Information Security Practitioners (ISPs) working in Norway. The primary target group of the UnRizkNow community is the ISPs working in the small, medium, and large enterprises. The

UnRizkNow community should be the target's group preferred venue for gathering and sharing information and knowledge in the InfoSec domain.

Project Key achievement indicators: The project employs some indicators to assess the usefulness of the UnRizkNow community. The objective of these indicators is to assess the knowledge sharing features of the UnRizkNow community according to the project objective. The indicator scales act as proxies for the degree of project achievements. The indicators are defined as follows:

1. *Fragmented information to Collected information*: It will be essential for the UnRizkNow platform to allow the members to capture and store InfoSec knowledge on the platform and assess it whenever they need it. Thus, the UnRizkNow community platform aims to reduce the fragmentation of knowledge on the community by allowing the members to collect the necessary information related to a given subject in one place.
2. *Outdated to Up-To-Date*: ISRM is not a static field, and it needs the knowledge of the latest methodology and strategy. Having outdated information on a given issue might not help the ISPs to address the issue effectively. Thus, it will be important for the members (ISPs) of the UnRizkNow community to receive and access the updated information on the community platform.
3. *Questionable trustworthiness to high trustworthiness*: It is imperative for the UnRizkNow community platform to provide information that the members can trust. The members may not tend to accept the knowledge having the questionable trustworthiness about its accuracy or credibility.
4. *Low relevance to high relevance*: The UnRizkNow community platform aims to provide knowledge that is highly relevant for the members in the context of the InfoSec issue they are trying to address.
5. *Difficult to find to easy to find*: The UnRizkNow platform will provide the possibility to access a wide range of knowledge available in the community. Therefore, it is important for the members to find the required information easily and immediately.
6. *Less secure to more secure*: It is imperative for the UnRizkNow community to provide secure knowledge sharing mechanism on the platform. It should be possible to share sensitive information with the intended members without compromising the security and privacy requirements.

1.1.1 Phases of the project

The activity of the project is distributed into four phases. The details of the phases and their objective, and the expected outcome are given below:

Phase I: Problem Identification: The first phase of the project deals with investigating the limitation of the existing electronic communities in the InfoSec domain. Further, it aims to explore the challenges faced by the community members while sharing InfoSec knowledge in such communities. The research will be conducted through literature review and quantitative analysis. The findings of the phase will be useful to get the initial insight into the determinants that influence the willingness to share knowledge on the communities of practice.

Phase II: Requirement and specification: The aim of phase II is to explore the findings of phase I further and establish a strong theoretical foundation of the identified problem. Furthermore, an investigation is performed to gather the requirement to establish a working electronic community of practice for ISPs working in Norway. Human-factors are desired to be explored to understand the underlying risks in establishing InfoSec eCoP. The outcome of this phase will explain the knowledge sharing preferences of ISPs and the validity of the result through the descriptive theories on knowledge sharing behavior.

Phase III: Development and evaluation: The objective of this phase is to establish the UnRizkNow platform using an online free tool. The knowledge sharing features of the UnRizkNow community will be developed according to the determinants identified in phase I & Phase II while the project achievement indicators will act as the validating tool to assess the applicability of the features. The phase will also focus on developing a secure knowledge sharing mechanism on the UnRizkNow platform. The outcome of the phase will be a prototype of the UnRizkNow platform which can be used and tested by the ISPs. Moreover, a conceptual framework will be produced which can be implemented in the later stage of the project.

Phase IV: Assessment (Future work): This phase aims to recruit ISPs in Norway to share knowledge on the UnRizkNow platform and observe the knowledge sharing activities for a given period (3-6 months). This task aims to observe the usefulness of the implemented knowledge sharing features on the platform. However, this phase is not implemented in the thesis as it required extra fund and time to recruit the ISPs and observe their behavior towards the knowledge sharing activity on the platform. This phase is archived for the future work, and more details are available in the future work section 6 of the thesis.

1.1.2 Architecture of UnRizkNow

Figure 1.1 presents the architecture of the UnRizkNow project. There are two fundamental components of the UnRizkNow architecture. The *technical* component assists in building the UnRizkNow platform to enable the knowledge sharing activities among the ISPs. The *social* component identifies the roles, sharing mo-

tivation, barriers, and incentives perceived by the members of the UnRizkNow community. The technical and social components create the container for the community. *Research methodology* focuses on setting the foundation of the research method, identifying the participants, collecting and analyzing data from the participants to realize the social and technical components of the project architecture. The components and sub-components of the UnRizkNow architecture are the foundation blocks for the research activities of the thesis. Article 1,5,6 investigate the technical component whereas Article 1,2,3,4,5 investigate the social component.

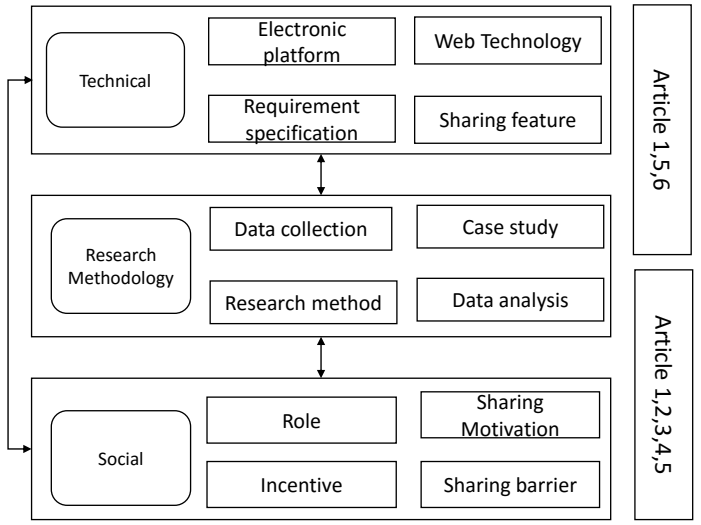


Figure 1.1: Architecture of UnRizkNow

1.2 Information Security Risk Management, Risk Assessment and Risk Analysis

Information is an essential asset for organizations, and information security (InfoSec) is an approach to maintain the confidentiality, integrity, and availability of the information [119]. Information Security Risk Management (ISRM) enables the information security technology to deal with the risks associated with the information [28]. Risk management is the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options. According to ISO Guide 73 [3], risk management is the set of systematic activities which are used to direct and control an organization about risk. Typically, risk management is used to represent the activities: context estab-

lishment, risk analysis, risk evaluation, risk treatment, monitoring and review, and communication and consultation. The steps of a risk management process differ widely, but to provide an insight into the risk analysis and management process, the guideline of ISO/IEC 27005:2011 [92] is followed.

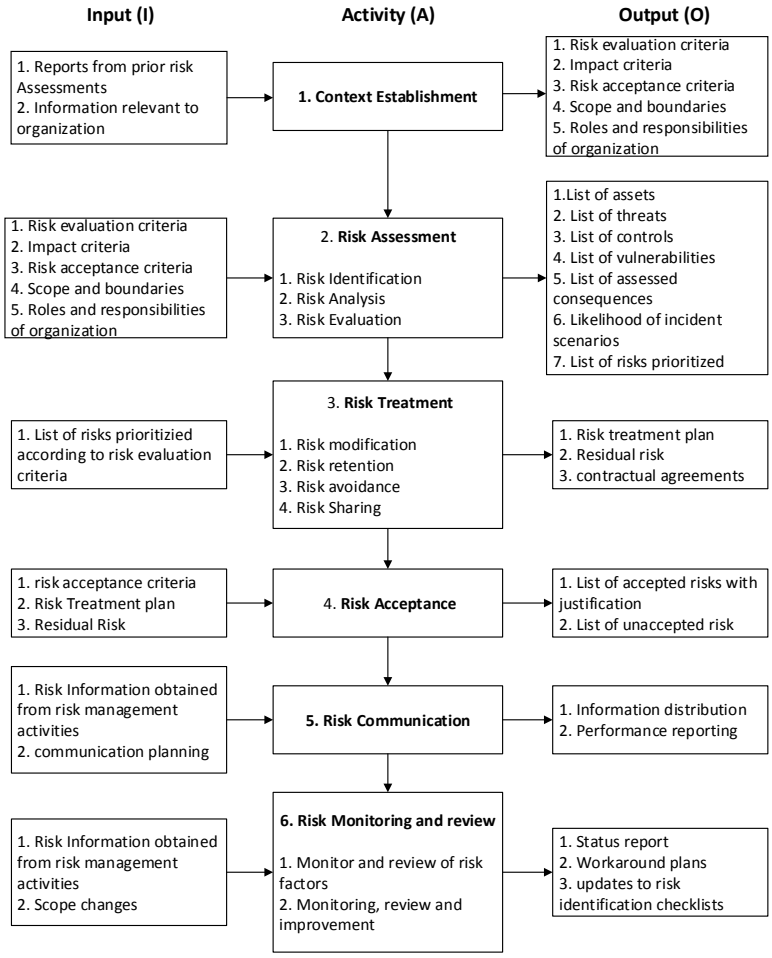


Figure 1.2: Overview of ISO27005 standard based on input, output of each activity, [5]

The representation of ISO27005 standard using the input and output at each activity is shown in the Figure 1.2. The first step consists of context establishment which includes determining the objectives of the organization, specifying the basic criteria (e.g., setting risk evaluation criteria, risk acceptance criteria), outlining

the scope and boundaries of information security risk management. The risk assessment consists of risk identification, risk analysis, and risk evaluation. The risk identification step starts with identifying the assets and their owners. Furthermore, the potential threats explored in association with the identified assets. Besides, the existing and planned controls, the vulnerabilities that might be exploited and a record of incident scenarios with their impacts related to those identified assets are also identified. Risk analysis step takes either qualitative or quantitative approach to assessing the consequences and the likelihood of occurrence of relevant incidents. In the risk evaluation step, the identified risks are prioritized according to the risk evaluation criteria about the incident scenarios that lead to those risks. The risk treatment options are selected when the result of the risk assessment step is satisfactory. Risk treatment options are selected based on the outcome of risk assessment, the expected cost of implementing these options and the expected benefits from these options. The risks are retained when the level of risk satisfies the risk acceptance criteria. Risk communication and consultation step ensure exchange/ sharing of information between the decision-maker and other stakeholders throughout the risk management process. Similarly, risks and their factors, i.e., the value of assets, impacts, threats, vulnerabilities and the likelihood of occurrence should be monitored and reviewed to identify any changes in the content of the organization at an early stage.

The representation of ISO27005 standard using the input and output at each activity is shown as a framework in the Figure 1.2. The details of the framework are available in [5]. The complete process in ISO27005 is presented into six fundamental activities (A1-A6). The first activity (A1), i.e., *Context Establishment* takes previous risk assessments report and other valuable information related to the organization, e.g., financial, budget planning, IT goals planning, resource requirements as an input and produces risk evaluation criteria, impact criteria, scope and boundaries, and different roles and responsibilities of the associated stakeholders in the organization.

1.3 Motivation and problem description

ISRM plays an essential role in securing the critical assets from potential risks. However, it is still a difficult task to identify and assess risks. The reason being the unavailability of enough data and cases that can help to build a robust assessment mechanism. The task of ISRM is usually carried out by ISPs or professional information security risk practitioners in an organization. ISPs face difficulty in selecting the appropriate RM method and establish a common understanding among the stakeholders involved in the RM tasks [143]. There is still a lack of a formal, structured way of collecting data, recording and reporting the activities involved in

the ISRM tasks [54]. ISRM activities require access to various information related to an organization. ISPs face difficulty sharing information related to ISRM processes due to the sensitive nature of the information. ISPs in different organizations often face the same challenges and employ a similar solution while often gathering and applying the same knowledge [57]. However, the individual approach to solve the challenge is inefficient as ISPs tend to invest extra time and effort [57]. The knowledge available, in the information security guidelines, best-practices documents, online ad-hoc groups, is inadequate to solve the professional challenges of ISPs [81]. Therefore, proper sharing and reuse of knowledge among the ISPs can improve the quality of ISPs work [185].

Recently, community-based online knowledge sharing method is proposed by several researchers [57], [175], [59] to enable InfoSec knowledge sharing among the ISPs. However, there is a significant challenge in establishing such electronic communities. The knowledge possessed by ISPs is highly valuable in solving critical tasks in infosec domain. ISPs may tend to hoard the knowledge in the absence of proper benefit of sharing the knowledge. Thus, it is essential for the eCOP to understand the preferences of the members of the community. The design of the knowledge sharing features should be based on the factors that motivate or demotivate the members to share the knowledge. There have been several studies [29], [95], [22] conducted to analyze the knowledge sharing behavior of members of the community. However, there is a still a lack of research work studying the factors that affect the ISPs to share their knowledge on community-based knowledge sharing platforms. Moreover, the presence of conflict in the interest among the stakeholders of electronic communities of practice may create undesired risks in the community. The risks generated due to a conflict of interest among the stakeholders have been studied previously in [188], [151]. However, there is an absence of studies to investigate the risks of eCoP due to the conflict in the interest of the community stakeholders. ISPs are reluctant to share their knowledge that contains sensitive information on eCoP [71]. The communities that fail to provide a secure way of sharing the knowledge of the member also fail to improve knowledge sharing practices [128]. The eCoP demands a novel way of sharing InfoSec knowledge without breaching the information security requirements.

1.4 Research Objectives, Questions, and Design

The thesis aims to achieve the following research objectives: First, establish a theoretical foundation for the study regarding the willingness of ISPs to share InfoSec knowledge on the community of practice. Second, develop an electronic community of practice (UnRizkNow) to enable InfoSec knowledge sharing. Third, improve and evaluate the UnRizkNow community. Figure 1.3 summarizes the flow

of research and approach to research questions. The research questions proposed in the study are stated as follows:

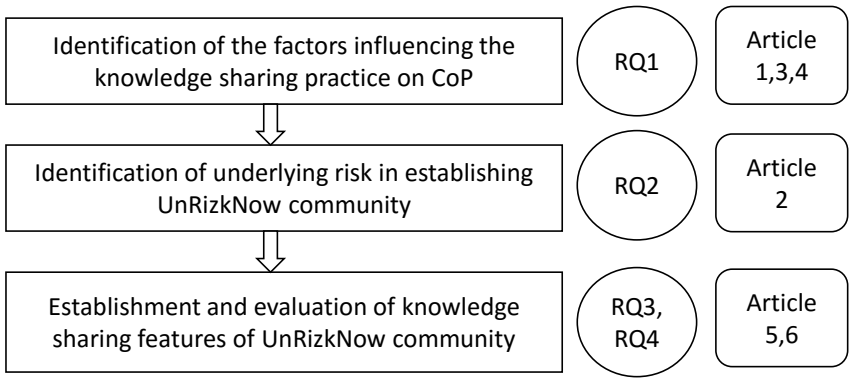


Figure 1.3: Research Flow, Research Questions, and Published Articles

Question 1: What are the factors affecting the willingness to share knowledge on the community of practice?

The CoP is a common way to engage professionals in sharing knowledge, discuss issues, and learn from others' experience to resolve several challenges in many organizations. The community members often tend to hide the information or not share with others if they perceive that the knowledge they possess is valuable and important. The purpose of this research question is to explore the descriptive theories to investigate the members' motivation towards sharing their knowledge on the electronic community of practice. Studies are conducted with the InfoSec bachelors students, professional IT members, and ISPs working in Norway to investigate this research question.

Question 2: What are the risks involved in establishing the UnRizkNow community due to the conflicting incentives of the stakeholders?

Establishing and maintaining InfoSec eCoP (UnRizkNow) is not a trivial task. There will be several stakeholders involved in the various activities associated with UnRizNow. The action of the stakeholders is often motivated by the incentives/ benefits perceived by them. The community may face the problem if there is any conflict between the incentives perceived by the stakeholders. Thus, it is imperative for the establishment of the UnRizkNow community to identify the underlying risks that can affect the normal operation of the community. This research question investigates the risks of the UnRizkNow community due to conflicting incentives of the stakeholders.

Question 3: What are the essential knowledge sharing features of the UnRizkNow platform?

There are several ad-hoc groups available on the internet dedicated to information security related topics. However, the existing online groups lack the active members who share relevant knowledge regularly. The knowledge available in these groups are not updated regularly, or the topic of the knowledge is irrelevant to most of the members. The UnRizkNow community can be useful in collaborating with the ISP and enabling the sharing of essential IS knowledge among them by addressing the limitations of the available ad-hoc groups. However, knowledge sharing is an intentional behavior which cannot be forced by someone [63]. Therefore, it is imperative to analyze the determinants that act as a motivation or barrier for the ISPs to participate in eCoP to share knowledge. This question investigates the factors that are essential to design the knowledge sharing features on the UnRizkNow platform.

Question 4: How can the sensitive knowledge be shared on the UnRizkNow platform?

Community members are often reluctant to take active participation in sharing their knowledge on the electronic community of practice [175]. People perceive that the knowledge that they possess may contain sensitive information. The level of participation and sharing activities can be diminished if UnRizkNow community fails to provide a secure way of sharing sensitive data. Thus, it is essential for UnRizkNow to allow sharing of InfoSec knowledge without violating the information security requirements. This research question investigates the novel approach to encourage sharing sensitive information on UnRizkNow.

1.5 List of included research publications

Article 1 [12]: Vivek Agrawal, and Einar Arthur Snekkenes. An investigation of knowledge sharing behaviors of students on an online community of practice. In Proceedings of the 5th International Conference on Information and Education Technology, pp. 106-111. ACM, 2017.

Article 2 [6]: Vivek Agrawal, Adam Szekeres. CIRA perspective on risks within UnRizkNow - a case study, IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 121-126

Article 3 [11]: Vivek Agrawal, and Einar Arthur Snekkenes. Factors Affecting the Willingness to Share Knowledge in the Communities of Practice. 23rd International Conference on Collaboration and Technology, CRIWG 2017, Saskatoon, SK, Canada, pp. 32-39

Article 4 [15]: Vivek Agrawal, Pankaj Wasnik, and Einar Arthur Snekkenes. Factors Influencing the Participation of Information Security Professionals in Electronic Communities of Practice. In Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Funchal, Portugal, pp. 50-60

Article 5 [13]: Vivek Agrawal and Einar Arthur Snekkenes. UnRizkNow: An open electronic community of practice for information security professionals. In Proceedings of the 2017 9th International Conference on Education Technology and Computers (ICETC 2017). ACM, New York, NY, USA, 191-197.

Article 6 [14]: Vivek Agrawal, and Einar Arthur Snekkenes. Secure Benchmarking using Electronic Voting. In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT 2018, ISBN 978-989-758-319-3, pages 25-40.

1.6 List of additional research publications

Article 7 [9]: Vivek Agrawal. Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard, Proceedings of Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016), pages 101-111, 2016.

Article 8 [10]: Vivek Agrawal. A Comparative Study on Information Security Risk Analysis Methods. Journal of computers 12.1 (2017): 57-67.

Article 9 [5]: Vivek Agrawal. A Framework for the Information Classification in ISO 27005 Standard. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 264-269

Article 10 [8]: V. Agrawal, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare," in Internet of Things. User-Centric IoT: First International Summit, IoT360 2014, Rome, Italy, October 27-28, 2014, Springer International Publishing, 2015, pp. 223-228.

Article 11 [105]: Thomas Kemmerich, Vivek Agrawal and Carsten Momsen, Chapter 10 - Secure migration to the cloud-In and out, In The Cloud

Security Ecosystem, edited by Ryan Ko and Kim-Kwang Raymond Choo, Syngress, Boston, 2015, Pages 205-230, ISBN 9780128015957

1.7 Scope of the Thesis

The main scope of the thesis is to investigate the issue of knowledge sharing in ISRM tasks. The focus of the thesis is to explore the role of InfoSec electronic community of practice in the knowledge sharing activities. The factors that influence the knowledge sharing activities of ISPs are studied and analyzed with the existing descriptive knowledge sharing theories. The scope of the thesis is limited to explaining the application, design, and significance of the UnRizkNow community in the information security domain. Furthermore, the thesis also develops a novel way of sharing Infosec knowledge securely on the UnRizkNow community. The intended audience of the thesis is the information security professionals and researchers in the InfoSec and the IT domain.

1.8 Thesis Outline

This thesis consists of three parts: the overview in Part I, the research articles in Part II, and the appendices in Part III.

In Part I, Chapter 1 presents an introduction of the thesis by stating the details of the UnRizkNow project, research problem and motivation, research questions, list of publications, and scope of the thesis. Chapter 2 presents the details in the form of background and related work knowledge that are essential to understanding this thesis. Chapter 3 presents an overview of the research methodologies that are adopted in this thesis. The chapter also presents an analysis of this thesis concerning the principles of Design Science Research Methodology (DSRM). Chapter 4 presents a summary of six peer-reviewed and published research articles. Chapter 5 describes the key contributions of this thesis. Chapter 6 underlines the topics and areas that are identified as the part of the future research activity. Chapter 7 presents the conclusion. In Part II, Chapter 8-13 includes six research articles selected to answer the thesis research questions and meet the research objectives. In part III, two appendices are presented; Appendix A gives more details about the technical code used in the thesis, and Appendix B presents four questionnaires used in the thesis to collect research data from the survey participants.

Chapter 2

Background and Related Work

This chapter is divided into two essential parts, i.e., background and related work. The background part of the chapter presents a summary of the fundamental concepts that are essential to understanding the overall topic of the thesis. It constitutes describing the essential concepts within information security and knowledge sharing. The related work part of the chapter presents the prior research work carried out within the given research area. The related work aims to establish a foundation for this thesis.

2.1 Information security knowledge sharing

Information security practitioners often face similar problems in IS domain, and it is expected of them to provide a proper solution to the problems. The extra resources can be saved by preventing the development of the same solutions [56]. Thus, knowledge sharing could also lead to solutions of better quality, as existing approaches could be advanced, instead of always developing the same solution. Knowledge sharing plays an essential role in the domain of information security due to its benefits towards the information security awareness of the employees. It is acknowledged that security awareness is the most critical factor needed to deal with the security incidents in organizations [157]. Information security knowledge sharing refers to collaboration with others by sharing the experience, ideas, and knowledge to protect information assets in organizations [59]. Thus, the establishment of knowledge sharing is vital as the individual knowledge possessed by information security practitioners is transformed into organizational knowledge. The knowledge is further transferred to end users and other stakeholders [59]. Knowledge sharing is essential to knowledge creation, organizational learning, and performance achievement [25]. Knowledge sharing is often treated as a normal func-

tion of workplaces as individuals in organizations have always created and shared knowledge [35].

Table 2.1: Types of knowledge, definitions, and examples in InfoSec domain adapted from [17]

Knowledge types	**Definitions**	**Examples**
Tacit	Knowledge is rooted in actions, experience, and involvement in specific context	Best means of dealing with customers
Explicit	Articulated, generalized knowledge	Knowledge of the security incident reporting.
Individual	Created by and inherent in the individual	Insights gained from information security risk management tasks
Social	Created by and inherent in collective actions of a group	Norms for communication on InfoSec community of practice
Declarative	Know-about	Which tools are appropriate to conduct penetration testing for a given system
Procedural	Know-how	How to administer the ISRM tasks
Causal	Know-why	Understanding why the vulnerability exists in the system
Conditional	Know-when	Understanding when to report an incident
Relational	Know-with	Understanding how the security compliance requirements affect the operational requirement of the business.
Pragmatic	Useful knowledge for an organization	Best practices, project experiences, information security frameworks

The terms information and knowledge are often used interchangeably in the literature [89]. The difference between the terms is discussed in [27], [47], [133]. According to Davenport et al. [47], "knowledge derives from information as information derives from data." Knowledge sharing is broadly classified into two groups, tacit and explicit [59]. Explicit knowledge sharing is the knowledge that can be articulated in words, codified, and transferred through a mechanism, acquired and accumulated. Codification of knowledge refers to the process of making knowledge accessible to those who need it [59]. Tacit knowledge can be thought of as

the know-how that is acquired through personal experience [134]. Tacit knowledge is more difficult to formally transfer as it resides in the minds of certain individuals and has not been codified in a structured form. According to Pai et al. [101], it is possible to share both tacit and explicit knowledge with the help of effective knowledge sharing mechanism. According to the taxonomy presented in [17], there are several other types of the knowledge in addition to tacit and explicit. The types of knowledge include social, declarative, procedural, causal, conditional, relational, and pragmatic. Table 2.1 summarizes different types of knowledge, definitions, and examples in the InfoSec domain.

In this thesis, knowledge refers to all intelligible ideas, information and data in whatever form in which it is expressed or obtained in the field of Information Security Risk Management [36]. Further, knowledge refers to all types of understanding gained through experience or study, whether indigenous, scientific, and scholarly [36].

2.2 Information security ontology and knowledge representation

Knowledge is represented in different ways in the computer science and InfoSec domains. People are searching for various means to absorb this different knowledge altogether, and not only the individual elements of information [51]. Ontology can act as the next step towards a better understanding by providing an explicit and semantically rich representation. Typically, ontology consists of entities, relation in between, and axioms restricting or enhancing the representations [69]. Many disciplines now develop standardized ontologies that domain experts can use to share and annotate information in their fields [136]. An ontology defines a common vocabulary for researchers who need to share information in a domain [186]. The term ontology comes from the Greek words *Ontos* (being) and *logos* (word). Ontology is defined as a formal, explicit specification of a shared conceptualization of common areas of interest [51], [131].

Figure 2.1 presents an ontology to capture core concepts of ISO27005 standard and relationship among them. The details of the methodology chosen to construct the ontology is given Appendix 14.1. The rational behind the ontology is structured as follows: Organization *has* Objective and *owns* some Assets. An Asset *hasSecurityProperty* named as CIA (Confidentiality, Integrity and availability). An Asset *has* some Vulnerability that *leadsTo* risk in the system, while a control *mitigates* the vulnerability. A risk *contains* consequence that *affects* Objective of Organization. A potential risk *harms* the organization. Event *has* a likelihood of occurrence and it also *modifies* consequence. Risk *isRealizedBy* Event in the system. A threat

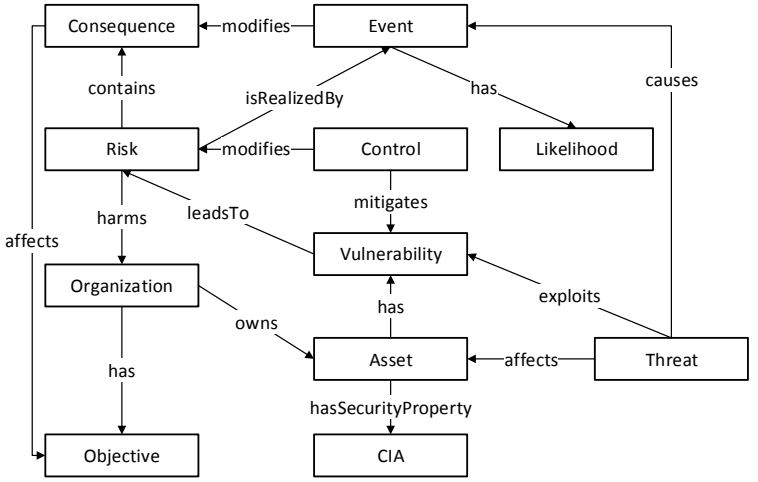


Figure 2.1: An ontology for ISO27005 standard [9]

affects an asset as it *exploits* the Vulnerability of the Asset and *causes* an event [1] in the system.

The dynamic nature of modern information security highlights the significance of sound security management. Information security practitioners deal with a variety of diverse security-related knowledge, e.g., the output of risk management tools, service level agreements. It is often an effort-consuming task, which has not yet been appropriately assisted by automated processes, mainly for large organizations [178]. Therefore, researchers proposed the importance of using an ontology to deal with the problems mentioned above in [162], [141]. Ontology provides a structured approach to support the process leading from simple statements found in policy to deployable technical controls [178]. Tsoumas et al. [178] define a security ontology as an ontology that elaborates on the security aspects of an information system. The authors have extended the Common Information Model [125] to address information security related concepts in a risk assessment perspective.

2.3 Knowledge sharing on Communities of Practice

The community of practice is a practical approach to implement knowledge sharing. The term 'communities of practice' (CoP) is introduced by Wenger et al. in 1998 [191]. Communities of practice [192] is defined as "*Groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen*

[1] An event is also known as security incident

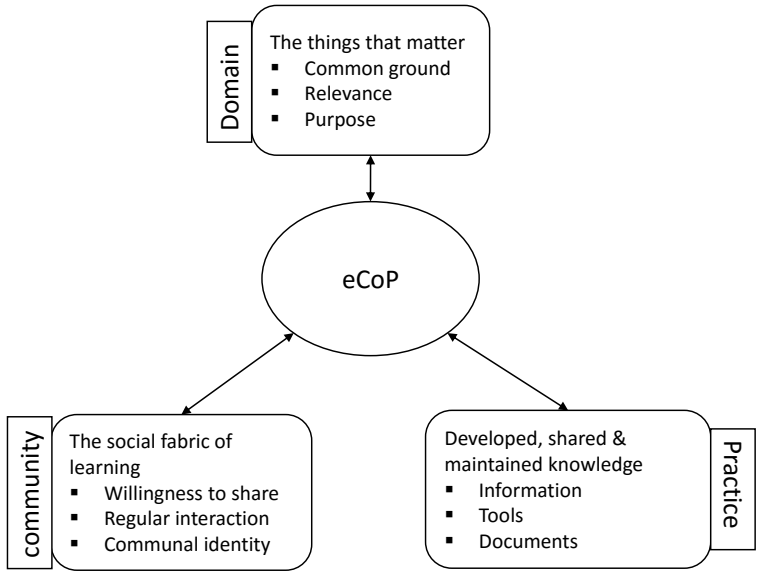


Figure 2.2: Structural model of electronic community of practice

their knowledge and expertise in this area by interacting on an ongoing basis." A CoP mainly consists of three fundamental elements: a) *Domain* creates common ground and a sense of a common identity. A well-defined (distinct) domain enables the community to understand its purpose and value to the members and stakeholders associated with the community, b) *Community* creates the bond among the members that enable the learning among them. A strong community can be developed when the members have mutual respect and trust among them. A strong community also encourages healthy interactions and discussion, c) *Practice* is the specific knowledge the community develops, shares, and maintains. A practice can be a set of ideas, tools, information that the community members share [192].

Table 2.2: Distinction between communities of practice and other structure, based on [192]

	Purpose	**Actors**	**Relation**	**Age**
Communities of practice	To create, expand, and exchange knowledge, and to develop individual capabilities	Self/selection based on expertize or passion for a topic	Passion, commitment, and identification with the group and its expertize	Evolve and end organically. It lasts as long as there is relevance to the topic and value and interest in learning together
Project Teams	To accomplish a specified task	People who have a direct role in accomplishing the task	The goals of the projects and milestones	The completion time of the project
Communities of interest	To be informed about a topic	Whoever is interested in the topic	Access to information and sense of like-mindedness	Evolve and end organically
Informal networks	To receive and pass on information, to know who is who	Friends and business acquaintances	Mutual need and relationships	Never really start or end. It exists as long as people contact each other

Figure 2.2 shows the details of the structural model of an eCoP based on Domain, community, and practice. The model provides a common language that enables discussion, collective action, and efforts to gain legitimacy [192]. It is always important to define domain, community, and practice to clarify the distinction of the community of practice from other such structures. There may exist many other communities to serve some purpose. However, they are not necessarily a community of practice. Similarly, not everything, which can be called as practice, gives rise to a community. Table 2.2 presents distinctions between communities of practice and other structure based on their purpose, who belongs to the community (actors), what holds them together (relation), and how long they last (age). The benefits of community of practice are highlighted into three distinct categories, i.e., *individual*, *community*, and *organization* [126], [60]. Individual benefits are perceived through improved reputation, increased levels of trust. Community benefits consist of increased idea creation, increased quality of knowledge, and problem-solving. Organizational benefits involve the most significant aspect - business values [169], [181].

Typically, a community of practice exists in either traditional (offline) or electronic form. Electronic communities use networked technology, mainly the internet [97]. The idea of having an electronic platform for the traditional communities of practice is supported in the studies [121], [194]. The traditional communities rely heavily on the location and have membership according to norms. The electronic communities of practice (eCoP) are organized around an activity, idea or task rather than location [97]. The electronic nature of the community provides the opportunities to facilitate communication among the members from different geographic locations and time zones. Electronic communities exist according to the identification of an idea or task, rather than location. They are formed and organized around activity and as a need arises [170]. It is also argued [163] that an adequate amount of knowledge is required to operate the online tools to facilitate eCoP objectives. Discussion forum, repositories, 'rooms' are to established to enable electronic communities.

2.3.1 phpBB

Online communities of practice can be instituted using tools. phpBB [144] belongs to the family of forum tools for building online community [171]. phpBB is a bulletin board tool written in the PHP programming language. phpBB can be utilized with the help of following items:

- The programming code to be executed
- A database to store information

- Web-server software as it is a web application
- A system (computer) to execute

phpBB is coded using the PHP server-side programming language, and MYSQL is one of the most commonly used databases to be used with PHP applications. phpBB can run on different operating systems and web servers, but it is commonly used on a Linux platform with the Apache web server. The reasons to choose phpBB to establish the electronic community of practice in this thesis are as follows:

- phpBB is free. The source code, plug-ins are available for free on the official website.
- phpBB is one of the most popular forum software. Thus, it will be easy for the users of the community to participate easily. Members do not have to learn an entirely new system.
- phpBB is mature. It was released on December 16, 2000. It has been around for more than seventeen years of active and heavy use [171].
- phpBB has rich feature and is open for custom feature additions. phpBB is equipped with numerous functions for customizing and operating the community.
- phpBB scales well as it performs under stress and can handle high post volume [50].
- phpBB enables account validation via user or admin action.

2.4 An overview of the theories defining the knowledge sharing behavior

Learning within a community is concerned with participation in the community-based activities of creating, sharing and co-construction of knowledge. However, the community members often tend to hide the information or not share with others if they perceive that the knowledge they possess is valuable and essential and if there is a low benefit of sharing. There are perceived benefits of contributing to the knowledge sharing process, but there are some real costs also. The distribution of benefits and costs are not often uniform in the community, and the community faces a problem that is also referred to as the tragedy of the commons [99].

Information security knowledge sharing is conceptualized through several descriptive theories:

1. *Theory of Motivation and Barriers (TMB)*: Ardichvili et al. [21] proposed the theory of motivation and barriers in 2003. Motivation represents the reasons for people's actions, needs, and desires. Motivation defines the direction and the reasons for a particular behavioral pattern. A major hurdle in knowledge sharing behavior is the lack of motivation. Furthermore, the role of intrinsic and extrinsic motivations is important in the domain of knowledge sharing organizations [34]. Extrinsic motivation meets the instrumental need of a human, i.e., money, financial reward, increase in the status. Intrinsic motivation is perceived by the values provided directly within the work [62]. Ardichvili et al. [21] mentioned in the study that employees feel the need to establish themselves as experts in the community. The sense of receiving recognition acts as a major motivation to improve the willingness to share their knowledge. On the other hand, members do not tend to share their knowledge as they are afraid that what they post may not be important or may not be correct.

2. *Theory of planned behavior (TPB)*: The theory of planned behavior is evolved from the theory of reasoned action. TPB describes the changes in human behavior based on the perspective of social influence. Intentions to perform behaviors of different kinds can be estimated from attitudes toward the behavior, subjective norms, and perceived behavioral control. Figure 2.3 depicts the theory in the form of a structural diagram. Attitude represents the predisposition toward the behavior in evaluations or appraisals. Subject norm refers to the extent of perceived social pressures regarding the execution of the target behavior. Perceived behavioral control is defined as the degree to which a person perceives that the decision to engage in a given behavior is under his/her control [95]. There are several studies [44], [157] that applied TPB in the domain of information system and security in recent years. The Theory of Planned Behavior was used to explain knowledge sharing behavior among the information security professionals in [175], [157]. A study [168] is also conducted to assess the behavior of employees towards complying information security policy through TPB approach.

3. *Social exchange theory (SET)*: Emerson et al. proposed the social exchange theory in 1976 [52]. However, the fundamental idea of social exchange theory is proposed by Homans et al. [82] in 1958. According to SET, individuals evaluate the perceived ratio of *reward* to *cost* and plan their actions to maximize their rewards [52]. In the community of practice setting, mem-

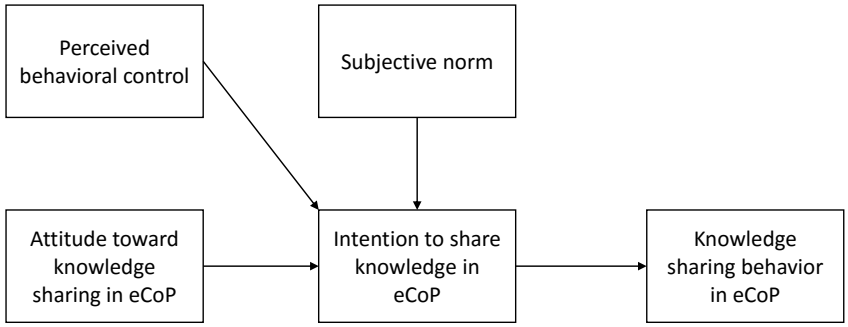


Figure 2.3: Structural diagram of Theory of planned behavior

bers of the community are willing to share the knowledge they possess when they perceive that they will also receive useful information from other members.

4. *Social presence Theory (SPT)*: Social presence theory is explored by Short et al. in 1976 [165]. The social presence is defined as, "degree of salience of the other person in the interaction and the consequent salience of the interpersonal relationships." It implies the degree to which a person is perceived as a 'real person' in mediated communication [70]. There are numerous studies [103], [42], [146] available that examine factors related to social presence in the traditional face-to-face classroom. In the context of learning in communities of practice, the presence of other participants as a 'real person' is important as it enables direct or indirect contact. The members of the community, therefore, indicate that they prefer to communicate with the trusted members [165].

Chapter 3

Research Method

The objective of this chapter is to provide a detailed information about the research methodology utilized in the thesis. The chapter starts with an overview of several research methods that are relevant to the domain of the thesis. The next section presents the argument to select the Design Science Research Method (DSRM) framework as the most suitable research framework to conduct the research. The objective of UnRizkNow project is explained using the concepts provided by the DSRM framework. The chapter concludes with the detailed explanation of the survey instrument used in the thesis.

3.1 An overview of the considered research methods

Research can be defined as a scientific and systematic search for pertinent information on a specific topic [107]. Redman and Mory [155] define research as a "systematic effort to gain new knowledge." The purpose of research is to discover answers to questions through the application of scientific procedures [107]. The basic types of research are as follows:

1. *Descriptive vs. Analytical:* Descriptive research deals with surveys and fact-finding inquiries of several kinds. The primary objective of descriptive research is to present the description of the state of affairs as it exists at present. The researchers dealing with this type of research mainly report what has happened and what is happening [107]. However, in analytical research, the researcher has to utilize the facts or information that are already available and analyze to make a critical evaluation of a particular scenario.

2. *Applied vs. Fundamental:* Research can be either applied (action) research or fundamental (pure) research [197]. Applied research targets finding a

solution for an immediate problem that the society or business organization is facing. The applied research aims to discover a solution for some critical practical problem. On the other hand, fundamental research is mainly concerned with generalizations and the formulation of a theory [197]. The primary aim of is finding information that has a broad base of applications and thus, adds to the already existing organized body of scientific knowledge [107].

3. *Quantitative vs. Qualitative:* Quantitative research is directed towards the measurement of quantity or amount. These methods usually rely on objective/subjective incident data and in the absence of sufficient statistical data they generally fail. Qualitative research is concerned with the phenomenon related to or involving quality or kind. Qualitative research aims at investigating the underlying motives and desires, using in-depth interviews for the purpose [107].

4. *Conceptual vs. Empirical:* Conceptual research relates to some abstract idea or theory. It is typically used to develop new concepts or to reinterpret existing ones. On the contrary, empirical research relies on experience or observation alone, often without any dependency on system and theory [107]. Empirical research is data-driven research, and it deals with conclusions which are capable of being verified by observation or experiment.

The discussion on types of research method also demands a discussion on handling the research data. The handling of the research data is covered into two main steps, i.e., research data collection and research data analysis. There are two main research approaches identified in the scientific research community, viz., quantitative approach and qualitative approach [130], [45]. The quantitative approach involves the generation of data in a quantitative form (numbers). The quantitative method, which includes intensive mathematical measures to model data for a complex environment, make the process more difficult. The qualitative approach is concerned with the subjective assessment of attitudes, opinions, and behavior. Qualitative methods do not use tools like mathematics and statistics to model the data, the result of the method is widely dependent on the ideas of people who participate in the research. There is a risk of giving subjective results while using a qualitative approach in data analysis. The qualitative method typically uses a scale as high, medium, or low to signify any magnitude.

The quantitative approach typically involves several modes to collect and analyze the data. **Survey** refers to the method of securing information concerning a phenomenon under study from all or a selected number of respondents [107]. Surveys

also require selecting populations for inclusion and analyzing results. Survey often uses standardized questionnaires or interviews [87]. A **questionnaire** is a written document including a list of questions to be distributed to some respondents. The questionnaire is distributed to the respondents either as a web form or a paper-based form. The paper-based form is an expensive and slow mode of distributing questionnaire as it needs manual processing to analyze the data. The questions in the questionnaire mainly fall under two categories, *open-ended* and *closed*. An open question is a question that has no predefined answers, and the respondents answer in their own words [96]. A closed question is a question for which the researcher has determined a set of permissible answers in advance [96]. Open-ended questions provide much information about the selected topics, but they are more difficult to analyze since they may cover a wide range of topics and need to be coded or grouped to provide some level of summary [87]. Scaled responses are also widely used in a closed question format. Scaled responses have some progressive order. Likert scale is one of the most frequently used scales in the research. In a Likert scale, the respondent is asked to respond to each of the statements in terms of several degrees, usually five degrees (but at times 3 or 7 may also be used) of agreement or disagreement [107]. **Interviews** are discussions, usually one-on-one between an interviewer and an individual (respondent) [73]. The aim of having an interview is to gather information on a specific set of topics. Interviews can be conducted in person or over the phone. Questionnaires are appropriate for collecting simple and straightforward information. Interviews are more effective for collecting complex and sensitive information [96]. **Focus group** is defined as a moderated discussion among 6-12 people who discuss a topic under the direction of a moderator [74]. The term focus in the title refers to the fact that the interview is limited to a small number of issues. The **case study** method is a prevalent form of qualitative analysis and involves careful and complete observation of a social unit, be that unit a person, a family, an institution, a cultural group or even the entire community. **Observation** is a data collection method, where a researcher directly observes phenomena [96]. Observation often acts as an alternative to survey and interview technique as it provides the researcher an opportunity to observe what the subject is doing directly. Observation technique helps to reduce the research bias often imposed by the respondents in the survey and interview-based techniques. **Extraction** is the collection of data from documents, records, or other archival sources [73].

3.2 Application of DSRM Framework

This research aims to solve an existing practical problem in the domain of knowledge sharing in information security risk management by creating an artifact in the form of an electronic community of practice (UnRizkNow). The problem is solved

Table 3.1: Application of DSRM Framework

DSRM Activities	**Activity Description**	**Knowledge Base**
Explicate problem	*What is the problem?* The existing eCoP fail to provide useful knowledge sharing features to the members. There is limited knowledge about the factors that influence the willingness of the members (ISPs) towards sharing their knowledge on the community of practice	Literature review, Online survey
Define requirements	*How should the problem be solved?* Identify the factors that explain the knowledge sharing preferences of the members on eCoP and establish UnRizkNow as the working eCoP for ISPs. Investigate the risks associated with the establishment of UnRizkNow community	Survey with ISPs, literature review of existing eCoPs, human-related risks
Design and Development	*Create an artifact that solves the problem* Establish the essential knowledge sharing features on UnRizkNow platform	Web technology, the survey with the ISPs in Norway
Demonstration	*Demonstrate the use of Artifact* Demonstrate how UnRizkNow can enable the knowledge sharing activities through the knowledge sharing features	Key achievement indicators of UnRizkNow project
Evaluation	*How well does the artifact work* Evaluate UnRizkNow in terms of providing essential knowledge to share features and encouraging knowledge sharing among ISPs	Use of eCoP in a given real-life case scenario, Key achievement indicators of UnRizkNow project

by applying creativity, innovation, and problem-solving capabilities. The created artifact would then be practically applied to improve the knowledge sharing activities in the ISRM practices. Thus, the research in the thesis lies in the domain of design science research in information systems. Design science research, which is popular in disciplines such as engineering and architecture, focuses on creation: ”how things ought to be in order to attain goals and to function”. The purpose of design is to change existing situations into preferred ones. [75] suggests that design science research should address either an unsolved problem uniquely and innovatively or a solved problem more effectively or efficiently. The aim of the design process in design science research is to create an innovative artifact. An artifact includes constructs (terms, notations, definitions, and concepts), models (abstraction and representation), methods (algorithms, process, guidelines), and instantiations (implemented programs) [96].

Table 3.1 shows the DSRM framework applied to the research topics of the thesis. The first column in table 3.1 lists the five activities that make up the DSRM as a nominal sequence. The second column further describes each of the activities in detail. The third column links the knowledge base with the different activities, i.e., how the activities are executed. The knowledge base provides the fundamental resources from and through which design science research is accomplished. It is composed of knowledge tools such as foundational theories, frameworks, instruments, constructs, models, methods, and instantiations [75].

3.2.1 A summary of sub-problems and method selection

Figure 3.1 shows the relationship among the research phase of the thesis, the research questions and the published articles, and a list of the applied research method to carry out the research phase. The details given in the figure provides a better understanding of the relevance of the articles and questions to the DSR activities along with the selection of the research methods.

Defining the problem(RQ1)

The initial studies in the thesis reviewed the existing literature to investigate the status of present eCoP regarding engaging the members in sharing useful knowledge. This activity resulted in a conclusion that there is a research gap in explaining the factors influencing the knowledge sharing practice on eCoP. In order to get more insight into the problem domain, this study further aimed to collect the opinion of the potential members of eCoP in Norway. The opinion of the members could be collected through the interviews or the questionnaire-based approach. The interview could result in a slow process of collecting data and with minimal sample size. Therefore, a quantitative approach was chosen, and a series

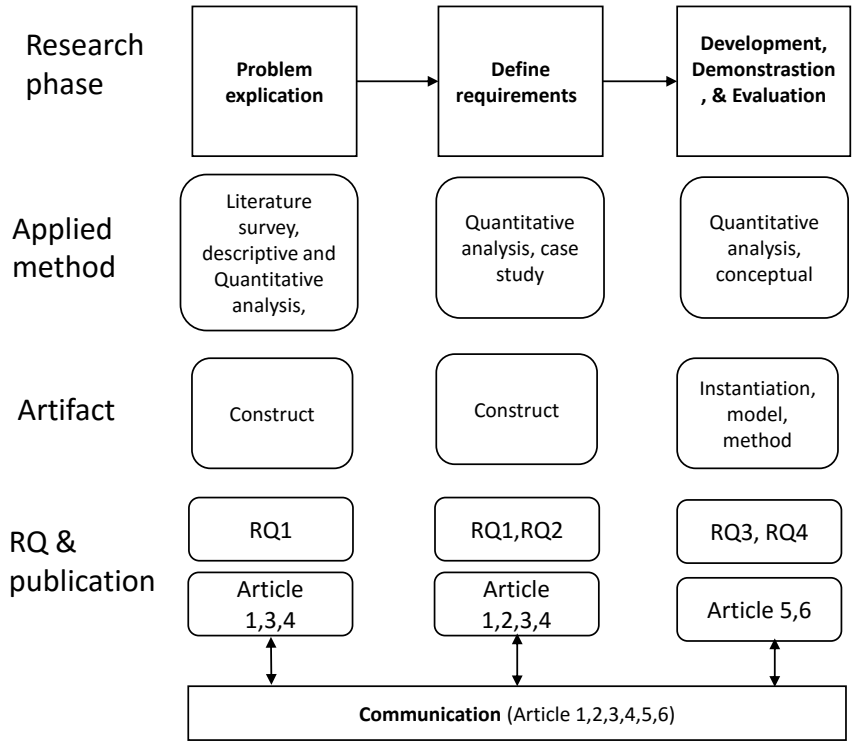


Figure 3.1: Research publication and their relationships

of surveys were conducted with the potential members of eCoP in Norway using the online questionnaire. Statistical analysis of the data was performed to calculate the descriptive statistics. The questionnaires were designed from the research work conducted in [95], [175]. The questionnaire had the multiple choice, Likert-type scales, closed-ended questions. The participants were recruited from three domains - the first batch of the participants was the InfoSec students studying at NTNU, Norway, the next batch of the participants were the IT professional working in universities and industries in Norway, and the third batch of the participants was the ISPs working as a full-time in Norway. The results from these studies provided the background for the next step in the research project.

Defining the requirements (RQ1 & RQ2)

The initial research helped to identify several factors that influence the willingness of the members to share their knowledge on the community of practice. However, it was still essential to validate the findings of the initial research with the help of already established descriptive theories in the domain. Therefore, several theories

explaining the knowledge sharing behavior of an individual and in a community setting were studied. The research revealed that the findings of the initial research comply with the well-known theories such as social exchange theory, the theory of planned behavior, social presence theory, and perceived trust theory. The next logical step would be to utilize these findings in establishing UnRizkNow as an InfoSec electronic community of practice in the project. eCoP often fail due to the conflict between the expectation of the community members [192]. Thus, the next goal was set to identify the risks generated from the conflicting incentives in UnRizkNow community. An online survey was conducted with the potential members of UnRizkNow in Norway to identify their roles and incentives perceived by them. There were very few risk analysis methods available that directly consider the human-factors in analyzing the risks in a given system. Therefore, CIRA was chosen as the most suitable candidate to investigate the conflict in the incentives between the *members* and the *organizer* of UnRizkNow, and mitigation plans were developed to address the identified risks.

Development, Demonstration, & Evaluation (RQ3 & RQ4)

The initial research conducted through RQ1 & RQ2 suggested that the survey participants were willing to participate in eCoP. However, they were reluctant to actively share as they were concerned about the sensitivity of the knowledge that they share. The research also highlighted that the participation of ISPs could increase if they get an assurance of receiving relevant information from the other members. Based on the findings of RQ1 & RQ2, it has been found that the present open electronic communities do not satisfactorily address the issues identified during the initial research. RQ4 & RQ4 explored the possibility of establishing an electronic community of practice for the information security practitioners. Therefore, an artifact, in the form of UnRizkNow community platform, was aimed to be developed in this phase of the research work. The UnRizkNow community would aim to correctly understand the concerns of ISPs and address them through the essential knowledge sharing features.

The initial research identified the issues faced by the ISPs while sharing their knowledge on eCoP. Therefore, it was essential to understand the preferred knowledge sharing features on such eCoP. The study further aimed to understand the ISPs perspective concerning the preferred knowledge sharing features on an eCoP. A quantitative approach was employed to carry out the further research, and an online questionnaire was created to communicate with the ISPs in Norway. A knowledge sharing model for the UnRizkNow community was developed to conduct the research work. The reliability of the model was evaluated based on the studies conducted in Article 1-4. The knowledge sharing influencing factors were compared and compiled together to identify their groups. The four groups, i.e.,

purpose, motivation, preference, and the facilitating condition, became the four elements in the research model. Besides, an online questionnaire was designed to cover the questions related to the elements and sub-elements of the knowledge sharing model. The participants of the online questionnaire were the ISPs working as a full-time employee in Norway.

The data collection activity revealed various factors that were imperative in establishing UnRizkNow community platform. A list of popular community building free tools (StackExchange, phpBB, AnswerHub) were explored. A feasibility study was conducted to understand the primary feature of the tools. The response from the ISPs and the project key achievement indicators acted as the guidelines to conduct the feasibility study. phpBB3 was selected as the best suitable to develop UnRizkNow community platform and knowledge sharing features were added to the platform as expressed by the ISPs through the online survey. The knowledge sharing features on UnRizkNow platform was evaluated against the five indicators established at the beginning of the project.

The latter part of this study focused on developing a novel approach to addressing security and privacy issues on eCoP. It has been identified during the initial research that the present benchmarking system in the InfoSec domain has a significant security limitation and privacy concerns. In answering the security and privacy limitation, a secure way of conducting the benchmarking on UnRizkNow has been proposed and evaluated in the thesis. The secure benchmarking system would enable knowledge sharing and encourage ISPs to participate more. Firstly, the security requirements of the secure benchmarking system were established in the study through the literature review process. Secondly, the security requirements of electronic voting were compiled through extensive literature review process. A model was developed to map the benchmarking protocol, structure, and concepts to electronic voting. The efficacy of the model was evaluated by performing security analysis and demonstrating the fulfillment of security requirements of the benchmark system. The feasibility of the model was evaluated by proposing the application of the secure benchmarking system on UnRizkNow platform. Theoretical arguments of cryptography and mathematical proofs were used to perform the evaluation.

3.2.2 DSR knowledge contribution framework

A design science contribution may fall into different domains. The contribution can be based on a new artifact that may bring a paradigm shift in the given domain. Additionally, a new artifact can be an improvement upon an established solution to a well-known problem. There is another form of the design science contribution that deals with using an existing artifact for a new purpose. Gregor and Hevner

[67] suggested that DSR contributions can be classified and positioned into two dimensions.

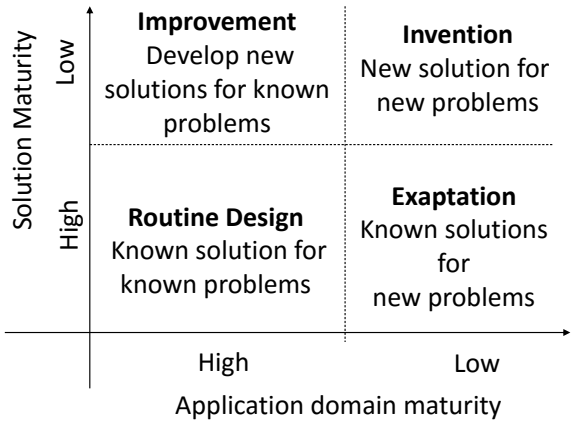


Figure 3.2: Design science contributions, adapted from [67]

Figure 3.2 presents a 2X2 matrix of research project contexts and potential DSR research contributions. The X-axis, i.e., Application Domain Maturity (ADM) shows the maturity of the problem from high to low. The Y-axis, i.e., Solution Maturity (SM) represents the current maturity of the artifacts from high to low that exist as potential starting points for solutions to the questions. The 2x2 matrix also identifies four kinds of design science contribution. A low ADM and low SM defines a new solution for new problems, and it is referred to as *Invention*. A high ADM and Low SM define new solutions to known problems, also known as *Improvement*. A low ADM and High SM indicates known solutions for new problems, also known as *Exaptation*. Finally, A high ADM and high SM indicates known solution for known problems, referred to as *routine design*. Unlike other entities of the matrix, the routine design does not have a major knowledge contribution. The contribution of the thesis is also presented in the alignment of the DSR contribution framework in the later chapter.

3.3 Survey instrument

The thesis used four questionnaires as the survey instrument to collect the data required in the Article 1-5. The list of the questionnaire is available in Chapter 15. This section presents an overview of the construction of survey instrument, testing of the instrument, ethical consideration, and evaluation of the used survey instruments in the thesis.

3.3.1 Questionnaire 1 [15.1]

This questionnaire was utilized in the study conducted in Article 1 [12]. The primary aim of the questionnaire was to collect the experience of the students while sharing knowledge on UnRizkNow platform. The response of the students would explain the knowledge sharing activities of the students observed during the course IMT1132. Firstly, a literature search was conducted to see what other studies have been done on the topic and determine how the previous studies researchers collected their data. The literature search showed that the questionnaires stated in [153], [24], [196] were highly relevant to assess the knowledge sharing activities of the students on the online platform. Thus, the existing instruments were adopted and modified according to the context of the present study.

The questionnaire was designed using the Google form and handed out to the students. The questionnaire, consists of 10 questions, was related to students' demographics, ISO/IEC 27005 and project work, use of web forum (UnRizkNow) and data sharing. The content of the questionnaire was evaluated and approved by the course instructor. The participation of the students was completely voluntary, and any student could choose not to participate without facing any consequence. A Likert-type scale was chosen to describe 'degree of agreement,' 'intensity of value' for several questions. The degree of agreement was described on a scale from 1 to 6. On this scale, selecting the 1 means that the statement was "Strongly disagree" and the 6 means "strongly agree." So students were asked to indicate how strongly they agreed with the statement on a scale from 1 to 6, with higher numbers indicating a stronger agreement that the statement was true. The intensity of value was defined on the scale of low, medium and high.

Though the data collection activity was satisfactory, there was a concern raised by the participants related to the use of third-party tool and server to store the responses. Participants and Course instructor expressed concern related to the use of Google form for the data collection purpose. This issue was addressed in the subsequent questionnaire development.

3.3.2 Questionnaire 2 [15.2]

This questionnaire was used in the studies conducted in the Article 2 [6] and Article 3 [11]. The primary aim of the questionnaire was to understand the willingness and barriers of the professionals in sharing knowledge on the community of practice. The questionnaire also had questions on the experience of participating on Community of practice, details of the role of the members, and the domain of the community. Firstly, a literature search was conducted to find other existing studies covering the stated issues. The questionnaire available in [98], [95] served as a

good starting point to formulate the questions for this study.

An online quantitative questionnaire was created using LimeSurvey. The survey was hosted on the project domain [7]. The survey comprised of 17 questions (39 questions including sub-questions) in total that assessed various aspects of information sharing and previous experiences with CoPs. The questions were discussed with the IT professional working in a Norwegian company to understand the relevance of the questions. The questionnaire was available in both English and Norwegian languages. Two native Norwegian language speakers translated the questionnaire from English to the Norwegian language. A 7-point Likert-type scale was used (1-Not at all, 7-Extremely) for evaluative questions, and lists of possible answers were provided for categorical questions. The reliability of LimeSurvey tool was tested using an automated code written in Java program. The exercise was aimed to ensure that even if a significant number of respondents access the questionnaire online, the web tool and server could handle the concurrent requests. The automated code is available in the appendix 14.2. The code was further used to generate a sample set of data and tested on SPSS for the reliability of the statistics.

A note on the privacy was added at the beginning of the survey to deal with the ethical issues. *"A note on privacy - This survey is anonymous. The record of your survey responses does not contain any identifying information about you unless a specific survey question explicitly asked for it. If you used an identifying token to access this survey, please rest assured that this token will not be stored together with your responses. It is managed in a separate database and will only be updated to indicate whether you did (or did not) complete this survey. There is no way of matching identification tokens with survey responses."*

3.3.3 Questionnaire 3 [15.3]

This questionnaire was used in the study conducted in the Article 4 [15]. The main aim of the questionnaire was to investigate the factors affecting the participation of information security professionals in eCoP in Norway. A literature search was performed to identify similar studies conducted in this domain. The search revealed the presence of questionnaires in the three articles [175], [95], [84] that cover the topic of this study very closely. Thus, the existing survey instruments were adopted and modified according to the context of the present study. Furthermore, a preparatory study was conducted to understand the survey designing principle based on the guideline given on [174]. The study started with the designing the primary questions that the questionnaire should address. The initial questions were as follows:

1. What are the tasks that they usually perform in their job responsibilities?

2. How do they obtain the necessary information required information that they need in their job responsibilities?
3. What are the challenges in obtaining the information?
4. To what extent does the community-based knowledge sharing activity increase the effectiveness of performing the job?
5. To what extent the ISPs are concerned to participate because of the privacy and sensitivity issues?

Afterward, the target audience was identified as the information security practitioners working in Norway. The population of information security professional in Norway was between 5000 and 10000 during the time the study was conducted. The study aimed to target 7% margin of error and 95% confidence level. Therefore, the sample size of approximately 130 was calculated to reach the goal. A dialogue was initiated with Information Security Forum (ISF)-Norway to survey with the live audience during their workshop. An online quantitative questionnaire was created using LimeSurvey open source survey tool. The questionnaire was posted on the project website [7]. The online survey was available in both English and Norwegian. The survey consisted of 18 questions covering the topics on demography, working activities, and preference for eCoP. The relevance of the questionnaire to the workshop members was examined and approved by the organizer of the ISF meeting. The reliability of LimeSurvey tool, server, and the database was tested using an automated code given in Appendix 14.2. The respondents accessed the online survey on their smartphone during the ISF meeting. Around 65 members of ISF attended the meeting, however, only 56 members participated in the survey. A note on the privacy was added at the beginning of the survey to deal with the ethical issues (as mentioned in Questionnaire 2). A provision was also added to the survey such that any participant can quit his/her participation at any point in time between the opening the survey link and be pressing the 'submit' button.

3.3.4 Questionnaire 4 [15.4]

This questionnaire was used in the study conducted in the Article 5 [13]. The primary aim of the questionnaire was to investigate the factors essential in designing UnRizkNow community for ISPs. The findings of Questionnaire 1-3 were used to formulate a knowledge sharing model based on four elements, i.e., purpose, motivation, preferences, and facilitating condition. Additionally, a literature search was conducted to explore the existing literature covering the research topic. The literature search activity identified [175], [71], [86], and [95] as the most relevant articles to formulate the questionnaire for the study. These studies used a very inter-related set of questions to evaluate the knowledge sharing practice in InfoSec and non-InfoSec electronic community. Thus, the existing survey instru-

ments were adopted and modified according to the context of the present study.

The target audience was identified as the information security practitioners working in Norway. A dialogue was initiated with the Information Systems Audit and Control Association (ISACA)-Norway chapter to survey with the live audience in their meeting. An online quantitative questionnaire was created using LimeSurvey open source survey tool. The questionnaire was posted on the project website [7]. The online survey was available only in the English language. The respondents accessed the online survey on their smartphone/tablet PC during the ISACA meeting. The survey consisted of 15 questions that assessed the demography, incentive, purpose, preferences for using eCoP to share IS knowledge. A 5-point Likert-type scale was used (1-Strongly disagree, 2-Disagree, 3-UnDecided, 4-Agree, 5-Strongly Agree) for evaluative questions, and lists of possible answers were provided for categorical questions. The 5-point Likert-type scale was chosen based on the study conducted in [175],[95]. The relevance of the questionnaire to the workshop members was examined and approved by the organizer of the ISACA meeting. The survey had the option for the respondents to decline their participation at any point in time if the respondents feel that the answers might breach their privacy. The questionnaire consisted of the following sections:

1. *Demography* - Information related to age, gender, job role, job locations, organization type, size of the organization, and hours spent on the IS tasks.
2. *Information security knowledge sharing* - information related to the purpose of sharing IS knowledge, preferences to share IS knowledge, incentive perceived during sharing, and attitude toward sharing IS knowledge on the electronic platform.

Chapter 4

Summary of Published Articles

This chapter presents the summary of six published research articles included in this thesis. The summary of the articles contains an overview of the problem statement, research methodology, and details of the key findings.

4.1 Article 1: An investigation of knowledge sharing behaviors of students on an online community of practice [12]

One typically expects that sharing and re-use of information improve both quality and process cost effectiveness. Thus, the UnRizkNow forum is developed to explore this assumption in a learning environment. The purpose of this study is to investigate the students' behavior in knowledge sharing activities on the UnRizkNow forum. The information security students of Bachelor's level course from the Norwegian University of Science and Technology (NTNU) are invited to participate in knowledge sharing activities related to ISRM course on the UnRizkNow forum.

An initial literature review was conducted to understand the knowledge sharing behavior of people in a community. A search string '*Knowledge sharing behavior*' was formulated to discover the relevant literature on the Google scholar. The studies published between 1990 and 2016 were selected to investigate the topic. The literature helped to identify the popular knowledge sharing theories, e.g., Social exchange theory (SET), social presence theory (SPT), the theory of planned behavior (TPB). Further, another literature search was conducted to study the knowledge sharing behavior of the students in the online communities of practice. Thus, '*knowledge sharing and students participation in the online community of practice*' was formulated to extract the relevant literature from Google scholar.

The studies published between 2000 and 2016 were selected to understand the current studies conducted to investigate the students' participation in the online community. The literature review activity helped to identify the relevance of the online community in the modern education field.

The UnRizkNow forum was integrated with a first-year Bachelor's course on risk management at NTNU. These students were selected because it was convenient (convenient sample) to recruit them for the experiment [58]. Students were assigned various risk analysis assignments and invited to share their knowledge as they worked on group assignments. Students were assigned into four groups, and the group membership stayed fixed for the duration of the course. Data collection was partially done from the knowledge sharing platform and partially done from a self-administered questionnaire.

The behaviors of students were monitored for six weeks during the course duration, and afterward, responses were collected through a questionnaire. The experimental part of the research focused on observing the behaviors of students toward knowledge sharing activities. Students and the instructor used the forum for eight weeks (from 1st April to 2nd June 2016). There were 37 posts, 19 topics and 42 users (37 students, 1 teacher, 1 member from the IT department, 1developer, 2 external users) as of 2nd June 2016. The key findings of this study are as follows:

- *Significance of UnRizkNow in sharing, learning and interacting:* According to Group 1, they found the UnRizkNow forum better for learning than sharing and interacting. Group 1 is the most active group on the UnRizkNow forum. They contributed more than 50% towards the content of the forum. Members of Group 1 used the forum to ask questions related to their assignment to seek answers from the others. We observed in our study that Group 1 used the concepts in their assignment report to solve the task. According to the course instructor, it enhanced the quality of their report. Figure 4.1 shows the distribution of values among the participating groups.

- *Factors affecting the use of UnRizkNow:* It has been observed during the experiment that the traffic was moderate on the UnRizkNow forum. Therefore, students were requested to participate in responding through an online questionnaire 15.1. Students responded that the UnRizkNow forum was introduced very late to them. Therefore, they had a low motivation to use the UnRizkNow extensively. A high number of members of each group answered that the forum was launched too late for their assignment. The second factor that demotivated them to use the UnRizkNow was the low return on Investment.

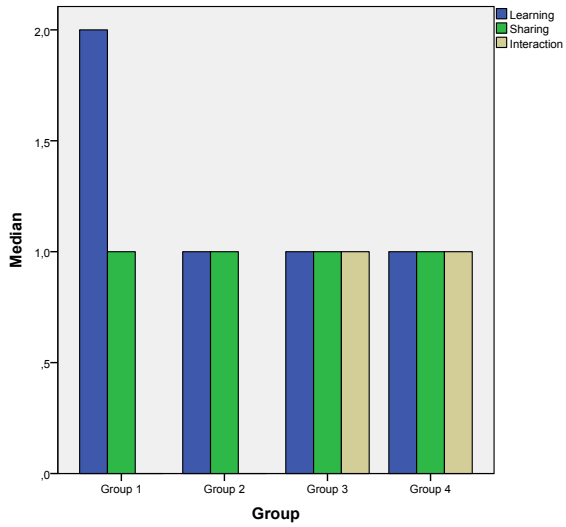


Figure 4.1: Significance of UnRizkNow in the context of learning, sharing contents and interacting with teachers according to participating groups

- *Validation of the findings:* The students used the UnRizkNow for learning, sharing and interacting with the instructor. However, students were skeptical of participating and sharing information for various reasons. The behaviors of students are explained with the help of descriptive theories at the individual and community level of participation.

  Individual level - *Social exchange theory (SET)* suggests that individuals evaluate the perceived ratio of benefits to costs and plan their actions to maximize their benefits [52]. The benefits can be expressed as money, respect, reputation or any other tangible incentives. In this study, students indicated that they failed to perceive the benefit of cooperating with other groups to share knowledge on the forum. According to the *Theory of Motivation and Barriers*, (TMB) [21] people are not always clear on what should be shared with other participants. They hesitate to share out of fear of criticism, or of misleading the community members. The response collected from the students confirm the validity of TMB in this setting.

  Community level - According to *Social Presence theory (SPT)* [166], the presence of other participants in CoP is important because it enables direct or indirect contact with others. the UnRizkNow is a relatively new forum with a few users (only 42 users altogether) to participate in the knowledge sharing activity. Hence, the UnRizkNow lacked in establishing a sense of social presence on the forum. According to the *theory of planned behavior*

(TPB) [16], more favorable attitudes toward a specific act, more favorable subjective norms, and greater perceived behavioral control strengthen the intention to perform the behavior. The study concludes that more the students are aware of the online presence of fellow participants, the more likely they will be engaged in the activities of the community.

4.2 Article 2: CIRA perspective on risks within UnRizkNow - a case study [6]

The UnRizkNow is an electronic community of practice in the InfoSec domain. It is imperative for the establishment of the UnRizkNow to identify the underlying risks that can affect the normal operation of the community. The learning that evolves from these communities is collaborative in nature, i.e., the collaborative knowledge of the community is more significant than any individual knowledge [115]. However, many CoPs have failed because the community stakeholders had either insufficient idea about the benefits/incentives of being involved in such communities or the incentives perceived by them are conflicting in nature. This article presents a study to carry out a risk assessment of conflicting incentives between the *members* and the *organizers* using conflicting incentive risk analysis (CIRA) method.

An initial study was conducted in the form of a literature review to investigate two primary issues, a) Identify the challenges in establishing the communities of practice, b) Identify the use cases where the CIRA method is applied. Therefore, '*failure and challenge in communities of practice*,' and '*a case study on "conflicting incentives risk analysis"*' are created as the search string to investigate the first and second issues respectively. The search strings were used to identify the literature published between 1995 and 2017. Google Scholar was used as the web search engine to identify the scholarly literature.

An online questionnaire 15.2 was created to assess the various aspects of information sharing and previous experiences with CoPs. A total of 52 respondents volunteered to complete all the sections of the online survey. Out of 52 respondents, 28 respondents have already participated in a CoP, whereas 22 members answered that they would want to join CoP. 2 respondents neither participated in any CoP nor they want to participate. The key findings of this study are as follows:

Identification of the utility factors: Based on the survey results the utility factors of the *members* are - *Improve knowledge:* the motivation to gain a better understanding about the domain knowledge, make use of the information shared by community members. *Share experience to help others:* refers to the intrinsic value

of sharing valuable experiences for the benefit of others. *Handling of privacy and confidentiality:* trust in the community and all stakeholders that the shared professional/private information is used confidentially and according to relevant privacy agreements. *Building reputation:* refers to the esteem, recognition received from others in the community, achieved by presenting relevant skills and competence in the domain. The utility factors that are considered to be relevant for the *Organizer* in the CoP setting: *Revenue:* Can be generated by collecting membership fees from members. A decision has to be made between increasing the number of members or setting a higher membership fee. Promoting the community among the professionals, securing money from the sponsors. By selling the knowledge/-technology designed in the community to third parties. *Reputation:* The Organizer is interested in establishing a better reputation in the business community.

operationalization of the utility factors: Table 4.1 illustrates the utility factors and their corresponding weights for both of the stakeholders, the four strategies identified as being capable of influencing these utility factors and their effect taking into account the utility factor's importance. In case of the *"Misuse of knowledge/information"* scenario the value is (-4, +2), for *"Diverting the purpose"* scenario (-5, +5), for *"Selection of inappropriate members"* (-9, +2), and for *"Improper incentive scheme"* (-4, -3). Scenarios 1-3 share the common characteristic that they all, to a different degree, can cause a potential loss for the community Member, while increasing the benefit of the Organizer. The fourth option is likely to result in avoidance by each stakeholder, as it would result in loss of utility for both parties.

Table 4.1: Overview of the incentives in relation to various strategies

			Influence of strategies on Utility Factors			
Stakeholders	**Utility Factors**	**Weights**	Misuse of the knowledge / information	Diverting the purpose	Selection of inappropriate members	Improper incentive scheme
Member	Improve knowledge	Very High	Unaffected (0)	**Decrease (-5)**	**Decrease (-5)**	Unaffected (0)
	Share experience to help others	High	Unaffected (0)	Unaffected (0)	**Decrease (-4)**	**Decrease (-4)**
	Confidentiality and privacy	High	**Decrease (-4)**	Unaffected (0)	Unaffected (0)	Unaffected (0)
	Build reputation	Medium	Unaffected (0)	Unaffected (0)	Unaffected (0)	Unaffected (0)
Change in utility			**-4**	**-5**	**-9**	**-4**
Organizer	Revenue	Very High	**Increase (+5)**	**Increase (+5)**	**Increase (+5)**	Unaffected (0)
	Reputation/ user satisfaction	Medium	**Decrease (-3)**	Unaffected (0)	**Decrease (-3)**	**Decrease (-3)**
Change in utility			**+2**	**+5**	**+2**	**-3**

Determination of risk: Risk is considered to be the result of the misalignment of the incentives between the strategy owner and the risk owner. In case of the *"Misuse of knowledge/information"* scenario the value is (-4, +2), for *"Diverting the purpose"* scenario (-5, +5), for *"Selection of inappropriate members"* (-9, +2), and for *"Improper incentive scheme"* (-4, -3). Scenarios 1-3 share the common characteristic that they all, to a different degree, can cause a potential loss for the community Member, while increasing the benefit of the Organizer. The fourth option is likely to result in avoidance by each stakeholder, as it would result in loss of utility for both parties.

Risk mitigation plan: The risk experienced by the Member when the Organizer is tempted to play either *"Misuse of knowledge/information"* or *"Selection of inappropriate members"* strategies can be mitigated by identifying other possibilities for revenue generation or by increasing the importance of the other relevant utility factor (Reputation / user satisfaction). In the case of *"Diverting the purpose"* strategy there are no other utility factors influenced on the strategy owner's side. Therefore, it is not possible to increase the weight of another utility factor. The risk could be mitigated by the introduction of an external regulator (e.g., Sponsor) being responsible for ensuring that the community is kept focused on the selected domain.

4.3 Article 3: Factors affecting the willingness to share knowledge in the communities of practice [11]

The purpose of this study is to investigate various factors that can affect the willingness of the IT professionals in Norway to share their knowledge in the open communities of practice. The study assumes that open communities of practice (CoP) can help to achieve the IT professionals in Norway to an optimal level of knowledge sharing. Therefore, the significance of communities of practice for the IT professionals is explored in this study. The findings of the study present various factors that increase or decrease the willingness to share knowledge on open communities of practice. These factors are further explained with the help of the descriptive theories. The findings of this study are useful to get the initial insight into the determinants that influence the willingness to share knowledge on the communities of practice.

An initial study was conducted with the help of a literature review to acquire the basic understanding of the area and identify the existing studies in the domain. A search string, *'willingness and barriers to knowledge sharing in the community of practice,'* was used to explore the relevant literature using the Google Scholar search engine. The literature available in English language and published between

1995 and 2017 were selected in the study. This exercise helped to understand how people perceive their knowledge in the community-based setting and the dilemmas associated with sharing the knowledge with others. Afterward, another study was conducted through an online survey 15.2 among the IT professionals working in Norway. The survey comprised of 39 questions which assess various aspects of information sharing and previous experiences with CoPs. A total of 52 respondents volunteered to complete all the sections of the online survey. The majority of the respondents were between the ages of 25-34 years (34.6%). The majority (about 76.9%) of the participants are affiliated with a university and industry. The key findings of this study are as follows:

Motivation and barriers to knowledge sharing: The study finds that having trust with the receiver of the information, and meeting the person face to face are the most critical factors that at as a motivation to share knowledge. The presence of a privacy policy that includes the detail about how the shared knowledge can be treated and used is also essential for the participants. The respondents also stated that an incentive (Useful knowledge, money, fame, reward) is necessary to encourage them to share knowledge.

The most significant barrier stated by the respondent was the breach of confidentiality. The participants of the community may share something that is very useful for the receivers, but at the same time can contain some sensitive information. The leakage of the confidential/ sensitive information can harm the individual. The concern of receiving irrelevant information from the others also lower down the willingness to share something useful with others.

Explanation of the findings: The survey results indicate the influence of social exchange theory (SET); people are concerned about the absence of any benefits to share knowledge. In this study, the survey participant indicated that they prefer to communicate with the trusted party, whether face-to-face (offline) or by any other means. The perception of the high degree of social presence and having direct or indirect human contact contribute to the building of trust. Thus, the effect of social presence theory (SPT) [165] in the setting of learning in communities of practice is visible. The respondents in the study indicated that the lack of security, leakage of sensitive information act as the most severe barrier to their knowledge sharing willingness on CoP.

4.4 Article 4: Factors influencing the participation of information security professionals in electronic communities of practice [15]

The purpose of this study is to contribute to a better understanding of the current status of the participation of the information security professionals (ISPs) in the electronic communities of practice (eCoP) in the information security (IS) domain in Norway. An initial study was conducted with the help of a literature review to acquire the basic understanding of the area and identify the existing studies in the domain. The literature identified in the Article 2 and Article 3 acted as the foundation block for the study. However, there was a need to understand the issues specific to the electronic community now. Thus, a search string, '*knowledge sharing in electronic communities of practice*' was formulated to explore the topic. The literature search was conducted on Google scholar and the literature published between 1995 and 2017 were selected for the study. This exercise helped to understand the knowledge sharing issues specific to the existing electronic communities of practice.

An online survey 15.3 was conducted, and the response of 48 respondents was used in the study. Based on the study and argument presented in the studies [116], logistic regression (also called as logit) was used as a statistical technique to formulate the results and findings. The probability of an ISP being a user of eCoP was tested with demographic data, nature of the job, and the knowledge sharing preference. Furthermore, the determinants of the knowledge sharing theories, i.e., the theory of planned behavior (TPB) [16], the motivation theory [62], and perceived trust theory [179] were used to test the statistical model.

The study finds that the number of employees in the organization, and working hours in the security area are the significant factors in predicting the participation in eCoPs. In addition, the extrinsic and intrinsic motivation is positively correlated with the participation in eCoP. The findings of logistic regression highlight that the participation of ISPs in eCoP is statistically influenced by the factor that other members of the community share relevant information to the problems of ISPs. In other words, high participation can be expected if the members of the community will share useful information with the participants. However, the tendency to share knowledge decreases when it is perceived that they are receiving irrelevant or not so useful information from other members. The application of TPB also led to some critical observation in this study. The probability of the participation in eCoP is significantly increased if the organization encourages the employee to participate in the knowledge sharing activities. Typically, eCoP needs information technology capabilities to establish the knowledge sharing process. The presence

of the necessary resources (in the form of platform, and service) also enables the ISPs to participate in eCoP.

4.5 Article 5: UnRizkNow - An open electronic community of practice for information security professionals [13]

The purpose of this study is to analyze the factors that are essential in designing the information sharing features of the UnRizkNow platform. The main objective of the UnRizkNow community is to involve the ISPs in knowledge sharing activities. The purpose of sharing knowledge in the community is to identify and solve the challenges faced by the ISP in the information security domain. The study conducted in the Article 1-4 served as a knowledge base for the study. However, a literature review is conducted to extract necessary information related to the information security community of practice. Thus, a search string, 'knowledge sharing in "information security" community of practice' is created to discover the existing studies through Google scholar. A research model, based on the *purpose*, *motivation*, *facilitating condition*, and *preference* towards sharing knowledge on the electronic platforms, is proposed in the study. Figure 12.2 presents an overview of the research model adopted in this study. The elements in the research model help to design the sharing rules, incentive schemes, and technical features of the UnRizkNow community. Additionally, an online questionnaire 15.4 is developed based on the elements of the proposed research model to collect responses from the ISP affiliated with ISACA Norway. The questionnaire consisted of 15 questions that assessed the demography, incentive, purpose, preferences for using eCoP to share IS knowledge. The response is utilized to design the most desirable features of the UnRizkNow community platform.

The study finds that the ISPs use electronic platform for both learning and educating. In other words, they want to share their knowledge with a purpose to solve the problems of other members as well as solve their own. The study also reveals that the ISPs' organization allow them to share their InfoSec knowledge outside the organization. The sharing of the knowledge is not restricted to the closed community. The current job role does not create any hindrance towards sharing the knowledge with others. The impact of the intrinsic motivation is more than the extrinsic motivation in encouraging the members to participate actively. In other words, ISPs want to build their reputation in the community by participating in the community-based knowledge sharing activities. The presence of any monetary benefits, i.e., rewards, promotion, and salary hike do not motivate the respondents to share their knowledge. ISPs are not willing to exchange their knowledge anonymously, and instead they want to see the identity of the members whom they are exchanging their knowledge.

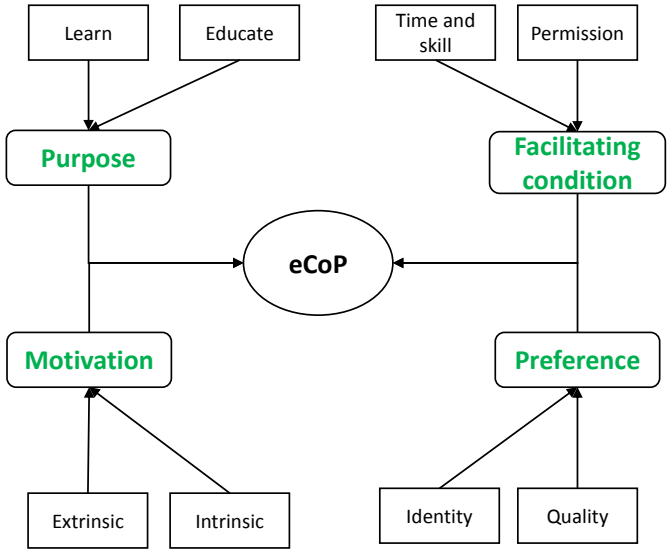


Figure 4.2: An overview of the research model based on purpose, motivation, facilitating condition, and preference

Furthermore, the knowledge sharing features were added on the UnRizkNow based on the responses collected from the ISP. The features of the UnRizkNow are designed such that the information accessible in the platform will help the members to search the information easily and quickly, get up-to-date information quickly, get more relevant content, establish reputation in the community, identify the members/post that is trustworthy, and get information in a more collected way.

4.6 Article 6: Secure Benchmarking Using Electronic Voting [14]

The purpose of this study is to design a secure knowledge sharing mechanism on the UnRizkNow platform. The goal is achieved by designing a secure benchmarking system using the concepts of the secure electronic voting system. It is a common practice in the industry to organize benchmark processes in establishing the standards for information security performance evaluation. A benchmarking system collects information security-related data from the organization to establish a standard. The information shared by the organization often contains sensitive data (details of the vulnerability, Cyber attacks). The present benchmarking systems do not provide a secure way of exchanging sensitive information between the submitter and the benchmark authority. The security limitation of current benchmarking

systems may hinder the sharing of valuable knowledge/information between the submitters and the benchmark authorities. There is a lack of any mechanism for the submitters to verify the final benchmark result contains the response submitted by them. Hence, ISPs are reluctant to take active participation in sharing their sensitive information in the benchmarking process. This study proposes a novel approach to solve the security limitations of present benchmarking systems by applying the concepts of electronic voting to benchmark. The solution provides secrecy to submitters' identity and the benchmark responses. The solution also ensures that all the submitted responses have been correctly counted and considered in the final benchmark result.

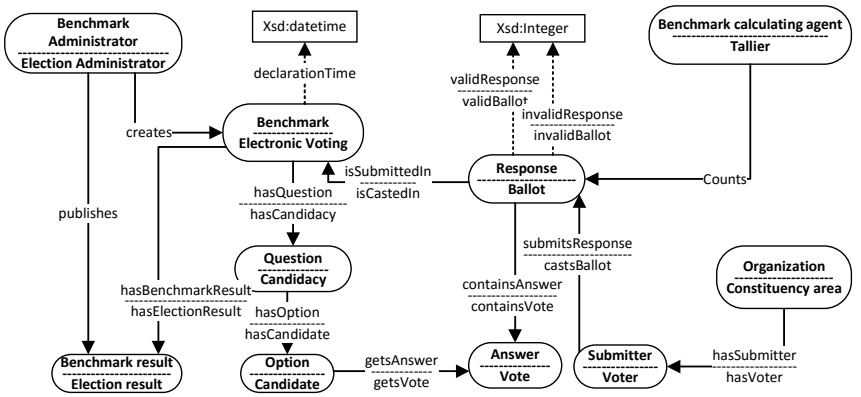


Figure 4.3: An ontology of benchmarking system and electronic voting system. The diagram shows that the concepts, actors, phases of benchmarking system can be mapped to electronic voting system.

This study presents the model of a benchmarking system that is typically used by an organization to establish the benchmark standard and provide the benchmark as a service. The study finds the security challenges that the current benchmark model face, and justifies a need to develop a more secure benchmarking system. The requirements of a secure benchmarking system are established in the study. Consequently, a novel approach is proposed to solving the security limitation of benchmarking systems by adopting the secure cryptographic proofs from the field of secure electronic voting. The security requirements of the electronic voting are established through a literature review. The details of the process of the literature review are presented in Section 13.5.3.

A mapping scheme is constructed to map the benchmarking system to the electronic voting system by mapping the protocol, the structure, and the concepts. Figure 4.3 presents an ontology to map the concepts of the benchmarking system

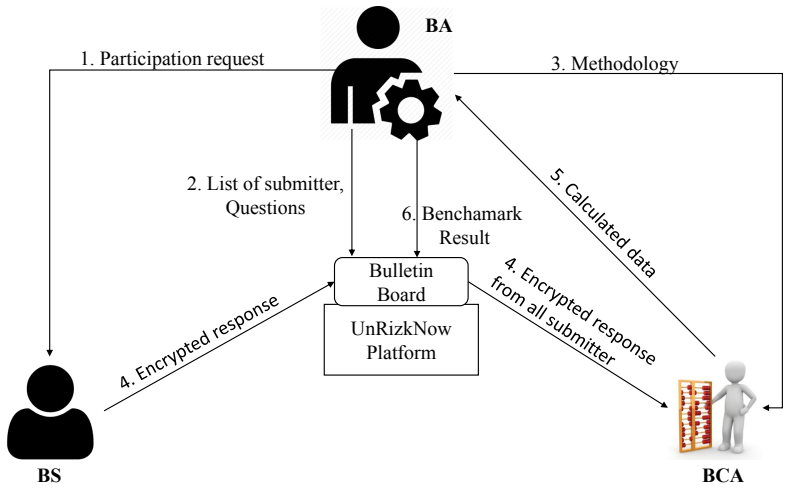


Figure 4.4: An overview of the benchmark model on the UnRizkNow portal

to the electronic voting system. It is also presented in how the different formats of benchmark question can be presented and how the benchmark result can be calculated using the concepts of electronic voting. The solution is based on the electronic voting protocol that provides secure transmission of the benchmark responses throughout the system. Furthermore, the identity of the response submitter is preserved by secrecy provided by the cryptographic protocols. The ISPs who participate in the benchmark process can ensure that their responses have been counted correctly while calculating the benchmark result.

Subsequently, a model is presented in the study to design a secure benchmarking system for the UnRizkNow platform using the concepts of the EV system. Figure 4.4 shows the various steps involved in carrying out the benchmark on the UnRizkNow platform. The study shows that a benchmarking system is more secure if it follows the EV system approach as it can satisfy the necessary security requirements.

To conclude, this chapter presented the research findings of the six research articles included in the thesis. The findings of the articles helped to investigate and implement phase I-III of the UnRizkNow project. Firstly, the factors that influence the knowledge sharing activities on eCoP were explored, and the descriptive theories on the knowledge sharing activities were identified. The survey, conducted with the InfoSec students, IT professionals, and the ISPs, showed the role of knowledge sharing determinants in understanding the knowledge sharing preferences on eCoP. Furthermore, the risk scenarios are identified through the analysis of the

human factors relevant in establishing the UnRizkNow community. Subsequently, the knowledge sharing features of the UnRizkNow community was developed according to the project key achievement indicators. Finally, a novel approach of conducting a secure benchmarking on the UnRizkNow community platform was proposed and evaluated.

Chapter 5

Summary of Thesis Contributions

This chapter outlines the research contributions within the knowledge sharing on the electronic community of practice. The chapter follows the sequence of the research questions and outlines each research question together with a summary of the contributions. The following sections describe the research contributions along with their evaluation using the DSR framework.

5.1 Insights into the knowledge sharing practice on the electronic community of practice

Question 1: What are the factors affecting the willingness to share knowledge on the community of practice?

This part of the research work contributes towards the goals of phase I and phase II (partially) of the UnRizkNow project. The thesis identifies the existing online ad-hoc groups which are not adequate to solve the challenges faced by the community members. The available groups lack in a proper understanding of the knowledge sharing requirements and preferences of the community members. Therefore, several studies are conducted to explore the factors affecting the willingness of the members to share knowledge on the community of practice. Article 1 [12] studies the knowledge sharing practice of the Bachelor's level student of information security program on the online platform. Article 3 [11] investigates different factors that act as a motivation for the full-time and part-time professional working in Norway to share knowledge in the community of practice. Article 4 [15] investigates the level of participation of ISPs on eCoP. The key contributions of these studies

are as follows:

1. Outlined the relevance of Theory of planned behavior (TPB), Social exchange theory (SET), Social presence theory (SPT), the theory of motivation and barriers (TMB), Perceived trust theory (PTT) in analyzing the knowledge sharing behavior of the members on the community of practice.
2. Identified various factors that act as a motivation or barriers to sharing knowledge on the electronic community of practice. The empirical study conducted with the InfoSec student, IT professionals, ISPs working in Norway supported the finding of the study.
3. A novel application of logistic regression is implemented to formulate the results and findings in the study conducted with the ISPs. The approach as mentioned above helps to predict the participation of ISPs on eCoP based on several factors. It is revealed in the study that both extrinsic and intrinsic motivation is positively correlated with the participation in eCoP. Further, the high participation can be expected if the members of the community share information that is useful to the participants. The probability of the participation in eCoP is significantly increased if the organization encourages the employee to participate in the knowledge sharing activities. The probability of participating in eCoP is not affected by the demography factors such as age, gender, and educational level.

5.2 Identification of human risks in the UnRizkNow community establishment

Question 2: What are the risks involved in establishing the UnRizkNow community due to the conflicting incentives of the stakeholders?

This part of the research work contributes towards the phase II of the UnRizkNow project. Article 5 [6] presents a study on the conflicts in the incentives of *member* and *organizer* of the UnRizkNow community of practice. The CIRA method is used to assess how the conflicts in the incentives perceived by members and organizer can disrupt the normal operation of the UnRizkNow community. The key contributions are stated as follows:

1. Identified the key utility factors of the members, i.e., Improve knowledge, share experience to help others, Handling of privacy and confidentiality, and building reputation. Identified the key utility factors of the organizers, i.e., Revenue and reputation.

2. The risk scenarios are determined based on the conflicts in the incentives perceived by members and organizers. Organizers can select inappropriate members for the community to increase the revenue (through member fee), but it would create the highest amount of loss interfering with the basic foundations of a CoP at the same time.

3. Developed risk mitigation plans to address the identified risk scenarios. For instance, 'Selection of inappropriate members' strategies can be mitigated by identifying other possibilities for revenue generation.

5.3 Establishment of the UnRizkNow community platform

Question 3: What are the essential knowledge sharing features of the UnRizkNow platform?

This part of the research work contributes to the objective of Phase III of the UnRizkNow project. The study contributes by establishing a working electronic community of practice using the phpBB3 [144] source code and designing the features of the community based on the requirements collected from the information security practitioners working in Norway. The essential features to encourage the participation and sharing of knowledge is studied in Article 5 [13]. The key contributions of this study are as follows:

1. Developed a research model to investigate the sharing rules, incentive schemes, and technical features of the UnRizkNow community. The research model has four elements, i.e., purpose, motivation, facilitating condition, preference.

2. Presented new insights into knowledge sharing requirements from the information security practitioners' point of view. The study finds that the impact of the intrinsic motivation is more than the extrinsic motivation in encouraging the members to participate actively. The presence of any monetary benefits, i.e., rewards, promotion, and salary hike do not motivate the respondents to share their knowledge. Further, the job role of ISPs does not create any obstacle in sharing the InfoSec knowledge on the electronic platform.

3. Established the UnRizkNow platform with the help of phpBB3 open source code. The platform enabled the participation of members and sharing knowledge on the UnRizkNow community.

4. Addressed the key achievement indicator (1-5) of the UnRizkNow project by adding several features to enable knowledge sharing on the UnRizkNow platform. The features enabled the functionality such as a) the information available in the community is easy to search, b) the updated information can be easily accessed, c) verify the information is coming from a reliable member, d) The information is relevant to the problem/concern of the member, e) all the useful information can be collected at the same place.

5.4 Novel solution to share sensitive knowledge on the UnRizkNow

Question 4: How can the sensitive knowledge be shared on the UnRizkNow platform?

This part of the research work contributes to the objective of Phase III of the UnRizkNow project. This study contributes to enabling secure knowledge sharing on the UnRizkNow platform by developing a secure benchmarking system. Article 6 [14] presents a secure benchmarking system for the UnRizkNow platform using the electronic voting approach. The objective of this study is to enhance knowledge sharing practice in the electronic community of practice. The key contribution of this study are as follows:

1. Established the current benchmarking model based on the literature review. This was the first time a detailed benchmarking model was presented. Identified the lack of the security requirements in the present benchmarking system. Completeness, uniqueness, universal verifiability, individual verifiability, eligibility, secrecy, soundness are identified as the requirements of the secure benchmarking system

2. Proposed a novel application of electronic voting to conduct benchmarking on the UnRizkNow platform. A new mapping scheme is created to map the protocol, phases, actors, structure of the benchmarking system to the electronic voting system. An ontology is constructed to map the concepts of the benchmarking system to the electronic voting system. This ontology acts as a tool to understand the concepts of the benchmarking system and the electronic voting system.

3. A benchmarking system model is proposed for the UnRizkNow platform. The non-receipt free K-out-of-L [79] voting protocol is used to establish the benchmarking protocol. An adversary model is constructed based on the *internal* and *external* attacker who can break the system. The details of

the trust in the system is formulated, and the proposed model is evaluated using the security metrics. The security proofs are derived from [79] to show how the model fulfills the security requirements - completeness, uniqueness, universal verifiability, individual verifiability, eligibility, secrecy, soundness.

5.5 Evaluation of artifacts and contributions within the DSR Quadrants

Evaluation is a primary and an essential activity in conducting Design Science Research [180]. This section identifies the types of artifacts [96] developed and evaluated based on the DSR evaluation framework. This thesis develops two constructs, one instantiation, one model, and one combined model and method artifacts. Table 5.1 summarizes the types of artifacts, objective of the artifact, research contribution, evaluation metrics [147] and evaluation method [96] chosen to evaluate the artifact. Figure 5.1 shows the placement of the contribution to the DSR knowledge contribution framework.

Construct1 (C1): C1 implements the objective of phase I and phase II of the UnRizkNow project. Construct C1 is proposed in Article 1 [12], Article 3 [11], Article 4 [15] to identify the role of eCoP in enabling the online knowledge sharing practice. The factors that may influence the knowledge sharing behaviors on CoP and eCoP are investigated with the help of InfoSec students and ISPs working in Norway. There are several factors in the form of descriptive theories identified in C1. The completeness and relevance of C1 are evaluated with the help of experts through online questionnaire and non-experts through experiments.

Table 5.1: Evaluation of artifacts

Artifact	**Objective**	**Contribution**	**Evaluation metrics**	**Evaluation method**	**UnRizkNow project**
Construct1 (C1)	Identify the factors influence the knowledge sharing practice on community of practice	Descriptive knowledge sharing theories	Completeness, relevance	Expert validation and evaluation	Phase I and Phase II
Construct2 (C2)	Identify the human-related risks in eCoP	Conflicting incentive risk analysis between organizers and members of eCoP	Efficacy, accuracy	Expert validation and evaluation, case study	Phase II
Model1 (M1)	Develop knowledge sharing model for InfoSec eCoP	A model based on purpose, motivation, facilitating condition, and preference	Accurcy, Completeness	Expert validation and evaluation, descriptive informed argument, demonstration	Phase III
Instantiation1 (I1)	Enable knowledge sharing activities for ISPs	UnRizkNow web platform established using phpBB	Design	Testing and observation, expert validation	Phase III
Method and Model1 (MM1)	Design a secure knowledge sharing mechanism for the UnRizkNow platform	Developed a secure benchmarking system for UnRikzkNow *Method*: Secure benchmark system *Model*: A mapping of benchmark to evoting	efficacy, feasibility	theoretical arguments, and mathematical proofs	Phase III

C1 construct addressed the problem of investigating the role of eCoP, and knowledge sharing behaviors of ISPs in Norway. The targetted problem is novel as it was never studied before. However, the adoption of eCoP as a solution to enable the online knowledge sharing practice is a known solution, and it has been used in several other domains [refer to section 2.3]. Thus, the contribution of C1 lies in the *exaptation* Quadrant of DSR knowledge contribution framework.

Construct2 (C2): C2 implements the objective of phase II of the UnRizkNow project. Construct C2 is proposed in Article 2 [6] to identify the human-related risks in eCoP. C2 investigates the conflicting incentive risks between organizers and members of eCoP using CIRA method. The evaluation of the C2 is done by expert validation and evaluation method and case study. The expert validation/studies identified the incentives of members and organizers of eCoP and case study presented the real scenario of using the UnRizkNow community as eCoP. The efficacy and accuracy of C2 are evaluated by identifying the risks and the treatment plans for the identified problems.

C2 construct addresses the problem of conflict between the incentives of organizers and members of eCoP. The problem raised here known in the community of practice domain. However, the solution in the form of application of the CIRA method to analyze the human-related risks is a new solution. Therefore, the contribution of C2 lies in the *improvement* Quadrant of DSR knowledge contribution framework.

Model1 (M1): M1 implements the objective of phase III of the UnRizkNow project. Model M1 is proposed in Article 5 [13] to enable knowledge sharing practice on InfoSec eCoP. M1 is developed based on knowledge sharing purpose, motivation, facilitating condition, and preference. The model is evaluated for its accuracy and relevance through the expert validation and evaluation and demonstration. The knowledge sharing requirements of the information security practitioners' are collected through an online questionnaire with the help of Likert scale type questions. M1 is further evaluated with the help of a demonstration by instantiating the findings in the form of working eCoP, UnRizkNow.

M1 model addresses the new problem of understanding the knowledge sharing preferences of ISPs on eCoP. The solution is developed based on several descriptive theories stated in section 2.4 and Construct C1. The nature of the solution is novel as it is suggested for the first time. Therefore, the contribution of M1 lies in the *invention* Quadrant of DSR knowledge contribution framework.

Instantiation1 (I1): I1 implements the objective of phase III of the UnRizkNow project. Instantiation I1 is proposed in Article 1 [12] and Article 5 [13]. A working

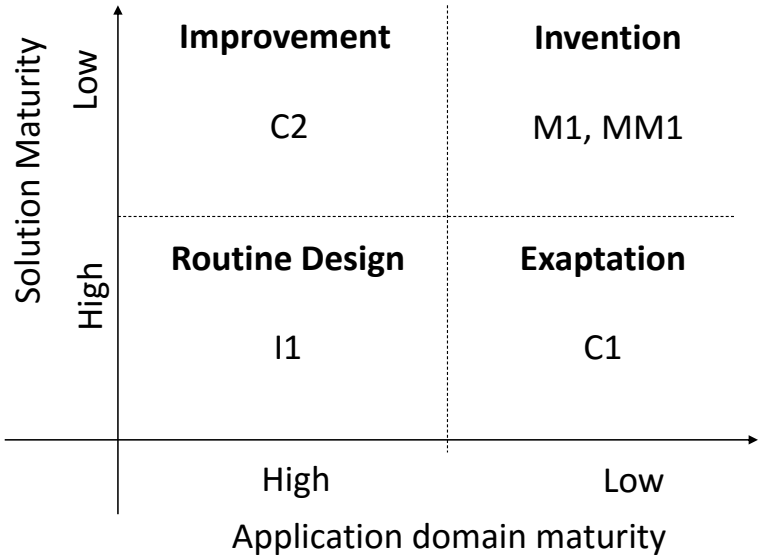


Figure 5.1: Identification of thesis contributions in DSR knowledge contribution framework

web platform using phpBB is established and used by InfoSec students to carry out an assignment. I1 is further modified based on the findings of model M1 to improve the search, reliability, update, importance, and structure of information on the UnRizkNow platform. The InfoSec students in the coursework evaluate the design of I1 through an experiment. The knowledge sharing activity of the students is monitored on the platform. I1 is further evaluated using testing and observation technique to check the functional and non-functional requirements.

I1 instantiation addresses the known problem of enabling knowledge sharing activities using electronic platforms. phpBB is adopted as the potential solution to meet the objective. phpBB is a well-known open source to establish eCoP. I1 is developed by making a minor modification to the available source code of phpBB. Thus, the contribution of I1 lies in the *routine design* Quadrant of DSR knowledge contribution framework.

Method and Model1 (MM1): MM1 implements the objective of phase III of the UnRizkNow project. MM1 is proposed in Article 6 [14] to improve sharing of sensitive knowledge among ISPs on the UnRizkNow platform. A secure benchmarking system is developed to collect and calculate benchmark from sensitive information shared by ISPs. A model is developed to map the benchmarking system to e-voting system to meet the security requirements of the benchmarking system.

The efficacy of MM1 is evaluated by performing security analysis and demonstrating the fulfillment of security requirements of the benchmark system. The feasibility of MM1 is evaluated by proposing the application of the secure benchmarking system on the UnRizkNow platform. Theoretical arguments of cryptography and mathematical proofs are used to perform the evaluation.

MM1 method and model addresses the lack of security requirements in the current benchmarking system. The proposed solution in the form of conducting benchmarking system as e-voting system is again a novel approach. It is shown that the security requirements of the benchmarking system could be fulfilled through e-voting approach. Thus, the contribution of MM1 lies in the *invention* Quadrant of DSR knowledge contribution framework.

To conclude, this chapter presented the details of the research contribution made in the thesis while exploring the research problem of the UnRizkNow project. The research contributions were categorized according to the research questions of the thesis. Additionally, the research contributions were mapped to the project phases to highlight the role of the contributions in achieving the thesis goal. Furthermore, the details of the artifacts and the evaluation method were explained using the DSR knowledge contribution framework. This exercise not only helped in identifying the characteristics of the research contribution but also in mapping the thesis contributions to the established knowledge contribution framework.

Chapter 6

Limitation and Future Work

This thesis investigated the factors that influence the members to participate in knowledge sharing activities on the electronic community of practice. The UnRizkNow community is established to solve the challenges faced by ISPs in ISRM practices through the knowledge sharing on UnRizkNow platform. The establishment of UnRizkNow community is in the early stage of development, and therefore, there are numerous possibilities available to improve the research in future. This chapter identifies potential topics for future work and the role of this thesis in supporting them.

6.1 Evaluation of knowledge sharing features

This thesis identified the influence of several well-known descriptive theories, e.g., SET, TPB, SPT, TMB towards the participation of ISPs in knowledge sharing activity on eCoP. The role of purpose, motivation, facilitating condition, and preference of ISPs while sharing knowledge is also studied. The study was primarily conducted through the online questionnaire with the respondents. However, the sample size of the study was low as less number of ISPs were available in Norway to participate in the survey. Due to the limited resources available in the project, a limited number of ISPs were involved in the project. The future work involves engaging more ISPs in Norway and outside Norway to participate in responding to the online questionnaire and improving the identified factors affecting the knowledge sharing activity. The features of UnRizkNow is designed such that the members can search the information easily and quickly, get the latest information quickly, get more relevant content, establish the reputation in the community, identify the members/post that is trustworthy, and get information in a more collected way. However, it was difficult to observe the usefulness of the knowledge,

extract from UnRizkNow platform, in solving the challenges faced by ISPs in the short duration. Thus, the knowledge sharing features proposed in this study will be evaluated by ISPs to understand the usefulness in the future study to address the phase IV of UnRizkNow project. The future work will involve ISPs on UnRizkNow community to report their problems/challenges and help to solve the problems.

6.2 Implementation of secure benchmarking on electronic platform

This thesis proposed a secure benchmarking system using the electronic voting concepts. However, the proposed benchmarking system is limited to conceptual analysis. Thus, the next important step is to implement the benchmarking system on UnRizkNow platform. The implementation on the platform will enable the members to share their knowledge in the benchmarking. Moreover, the performance of the secure benchmarking system can be evaluated. The current study is limited to the theoretical analysis of the proposed solution. The UnRizkNow platform is established on phpBB open source platform which uses the PHP server-side programming language. There has been already many existing e-voting tools available written in PHP language. The mapping of the benchmarking system to e-voting system will act as the guiding tool to implement the proposed benchmarking system on UnRizkNow. There is also a concern related to the network performance issue of the proposed benchmarking system. The size of the response can grow intensely with the questions and a large number of benchmark submitters.

6.3 Electronic Community of Practice in Healthcare

The investigation of the role of the electronic community of practice is identified in the InfoSec knowledge sharing among ISPs in this thesis. The ISPs, who participated in this study, belong to different industrial sectors in Norway. The future effort will be directed to involve ISPs associated with the healthcare sector in Norway. During the study, it has been identified there is a tension between the operational requirements and InfoSec compliance requirements in the healthcare sector. The tension often leads to an inefficient outcome in the health and care service. Therefore, it is essential to understand the challenges/dilemma from the perspective of the frontline staffs (Doctors, nurses, IT logistic personnel) and information security officers involved in the health and care service, and help them find good resolutions for their problems. Initially, an investigation of the existing methods available to the medical practitioners to capture and share the information related to security and privacy challenges will be conducted. The objective of this study is to establish an electronic community of practice (eCoP) to understand the

challenges raised by the information security compliance requirements of Healthcare. The potential members of the community will be any staff member who is associated with health and care service in Norway.

Chapter 7

Conclusion

The thesis conducted research work to implement the objective of UnRizkNow research project. Phase I, Phase II, and Phase III are attained in the thesis through four research questions and six peer-reviewed research articles. The thesis emphasized that sharing of knowledge among ISPs is essential to solving the challenges that they face in conducting ISRM practices. Thus, the establishment of UnRizkNow community is proposed to enable knowledge sharing activity among the ISPs. UnRizkNow community platform is constructed using phpBB3 open source code to support forum-based discussion among the community members. The knowledge sharing activity in the community was initially studied with the information security bachelor's students in NTNU. The study revealed that the students used UnRizkNow for learning, sharing and interacting with the instructor. The study also showed the evidence of the knowledge sharing behavior of students is in compliant with the established descriptive theories, e.g., SET, TMB, SPT, TPB. Though the students are not intended users of UnRizkNow community, an initial experiment with the students helped to identify various factors that act as a motivation and barrier in the knowledge sharing activity. The experiment with the students also helped to discover the existing knowledge sharing theories to explain the knowledge sharing behaviors on community-based learning. The findings of the study were later applied and studied with the IT and InfoSec professionals working in Norway. A series of online survey was conducted with the potential members (ISPs) of UnRizkNow community to understand to present level of their participation on eCoP. The factors, which are significant in deciding if the members (ISPs) would participate in knowledge sharing on UnRizkNow, were also studied. Logistic regression is used as a statistical technique to formulate the results and findings. The findings of logistic regression highlighted that the participation of

ISPs in eCoP is statistically influenced by the factor that other members of the community share relevant information to the problems of ISPs. The probability of the participation in eCoP is significantly increased if the organization encourages the employee to participate in the knowledge sharing activities. The study revealed that participation of ISPs, who work full-time or more in performing InfoSec tasks, is low on eCoP. Further, the study also revealed that ISPs tend to participate in eCoP if other members of the community share relevant information. There was a strong influence of the determinants of TPB theory (i.e., subjective norm, and perceived control behavior) on the participation of ISPs on eCoP.

The thesis learned the preferences of ISPs towards sharing their sensitive and valuable knowledge on eCoP. A research model based on the purpose, motivation, facilitating condition, and preference is developed to investigate the issue. A study was conducted with the ISPs in Norway through an online questionnaire. The number of respondents was not very high. However, all the respondents were affiliated as a full-time ISPs working in Norway. Thus, the answers provided by the participants were used in the scope of the thesis. The study showed that members are not willing to share their knowledge anonymously when they interact with other members. A significant number of respondents agreed that their organization does not create any hindrance in sharing their knowledge outside the organization. Based on the data collected from the ISPs, several features were added to UnRizkNow platform such that the information accessible to ISP will experience an improvement in search, update, reliance, importance, and structure. Furthermore, the thesis proposed a secure knowledge sharing mechanism on UnRizkNow platform. The study showed that the present InfoSec benchmarking system lack security and privacy mechanism. Thus, the present benchmarking approach to vulnerable to several security flaws. The thesis proposed a novel approach to conduct secure benchmarking using the concepts from the electronic voting domain. The study proved that the concepts of benchmarking could be mapped to secure electronic voting concepts while addressing the security limitations of the benchmarking system. The proposed solution enabled the benchmark submitter to participate and submit their responses without disclosing their identities and revealing the content of the response. A demonstration is presented to incorporate the secure benchmarking system into UnRizkNow platform. The secure way of conducting benchmarking can encourage knowledge sharing activity on UnRizkNow platform.

Part II

Published Research Articles

Chapter 8

Article 1: An investigation of knowledge sharing behaviors of students on an online community of practice

Agrawal, Vivek, and Einar Arthur Snekkenes. "An investigation of knowledge sharing behaviors of students on an online community of practice." In Proceedings of the 5th International Conference on Information and Education Technology, pp. 106-111. ACM, 2017.

8.1 Abstract

One typically expects that sharing and re-use of information improve both quality and process cost effectiveness. To explore this in a learning environment, we have developed the UnRizkNow forum. The purpose of this study is to investigate the students' behavior in knowledge sharing activities on UnRizkNow forum. In our study we found that students used UnRizkNow for learning, sharing and interacting with the instructor. However, students are skeptical of participating and sharing information for various reasons. The behaviors of students are explained with the help of descriptive theories at the individual and community level of participation. The findings of this study will assist teachers and researchers to predict the behavior of the participants in an online community of practice and to assess the effectiveness of design alternatives when developing knowledge sharing platforms for learning information security.

8.2 Introduction

Over the past decade, the rise in the information and communication technologies has changed the face of learning environment and processes for everyone. The focus of learning is strongly shifting towards online community-based modes of training for students in higher education [49]. Social networking websites like Facebook, Google plus, web forums like StackOverflow, wiki, blog have become popular among the students as online learning communities [108]. The use of such online learning communities is gaining popularity for educational purposes among students and teachers [99]. However, learning within a community is concerned with participation in the community-based activities of creating, sharing and co-construction of knowledge [49]. Students may not want to share their ideas, skills with others due to inadequate understanding of the benefits/incentive of doing so, while others may not have enough time to share their experiences or to learn how to use the available information systems. The issues like confidentiality and privacy can also affect the level of participation and knowledge sharing activities on the online learning platform. The contents shared by students can reveal some sensitive information, or it can make everyone aware of the students' skills and secrets of their competitive edge. Since access to the public online community is not restricted to contributors only, there is a temptation for students to enjoy the resource without contributing anything useful to the community [33]. There are surely perceived benefits of contributing to the knowledge sharing process, but there are some real costs also. The distribution of benefits and costs are not often uniform in the community, and the community faces a problem that is also referred as *tragedy of the commons* [33]. Considering the potential cost and benefits of sharing knowledge with others, some individuals may feel to hold themselves from sharing what they know [33]. According to Davenport et. al. [47], *"knowledge derives from information as information derives from data."* In this study, knowledge refers to all intelligible ideas, information and data in whatever form in which it is expressed or obtained in the field of Information Security Risk Management [36]. The terms *information* and *knowledge* are often used interchangeably in the literature in the context of sharing.

UnRizkNow [184] is a Norwegian-based Online Cyber Security Risk Management Community of Practice (CoP) for Cyber Security Risk Management (CSRM) practitioners. The objective of UnRizkNow is to identify relevant challenges that CSRM practitioners face in their field of interest and enable them to resolve these challenges by sharing knowledge in the form of ideas, answers, and experience. The proposed CoP is in the early phase of development and needs elaborate research in several areas to establish it as a preferred tool for gathering and sharing information and knowledge in information security area. We believe that the ini-

tial research with the information security students will give us useful insights to understand the behaviors of participants towards knowledge sharing tasks on UnRizkNow. These findings can be used to enhance the knowledge sharing features of UnRizkNow and test it with cybersecurity practitioners afterward. The following research questions are specified to attain the objective of the study:

RQ1 What are the prevalent behaviors of information security students towards knowledge sharing activities and how can existing descriptive theories explain these behaviors?

This paper contributes to our understanding of knowledge sharing behaviors of students in several ways. The information security students of Bachelor's level course in Norwegian University of Science and Technology (NTNU) are invited to participate in knowledge sharing activities related to information security risk management on UnRizkNow. We monitored the behaviors of students in an experiment and collected their responses through a questionnaire. The experimental part of our research focuses on observing the behaviors of students toward knowledge sharing activities. Our study provides new insight into the explanation of student sharing motivation and behavior. We believe that this insight is essential when improving our current state of sharing. The rest of the paper is structured as follows: In section 8.3, the theoretical foundation of knowledge sharing and students' participation in the online community of practice is presented. In section 8.4, the research approach of the study is explained. In section 8.5, the findings of this study is explained. Finally, the paper ends with a discussion of the results, limitation and expected future work, and the conclusion.

8.3 Related Work

The first part of this section presents a review of the literature giving an overview of knowledge sharing and several issues related to it. We then review current work on the students' participation in the online community of practice and increase in the use of social media in the process of learning.

8.3.1 Knowledge sharing

According to Davenport [46], knowledge sharing is a voluntary act. Sharing implies a conscious act by an individual who participates in the knowledge exchange even though there is no compulsion to do so. Davenport also states that knowledge sharing often becomes unnatural. People tend to hide the information or not to share with others if they perceive that their knowledge is valuable and important. Therefore, the motivation that can affect an individual's decision to share

knowledge becomes significant [29]. Gagné [63] presented a model of knowledge-sharing motivation based on a combination of the theory of planned behavior (TPB) and self-determination theory (SDT). He argues that more positive attitudes toward knowledge sharing can be achieved out of interest or personal meaning. He also states that empowerment is related to the follower's needs for competence, relatedness, and autonomy, which are essential conditions for effective knowledge creation and innovation. Many organizations are investing significant money and time into knowledge management initiatives [187]. Many experimental studies are showing that institutions can save their investment expenditure if sharing security-related knowledge [117]. However, it has been estimated that at least $31.5 billion is lost per year by Fortune 500 companies as a result of failing to share knowledge [23]. Cabrera et al. [33] studied several difficulties that an organization face in encouraging its employees to share knowledge with co-employees and presented several knowledge-sharing dilemmas.

8.3.2 Students' participation in the online community of practice

Online social media is gaining popularity among college students [100]. Students are also adopting social media to share their knowledge, engage themselves asking questions and helping other students [153]. Teachers are also adopting social media to reach out to their students easily [123]. Online discussions can contribute to the development of students' critical thinking skills [24]. An Online community of practice enables students to take active participation in the discussion at a time convenient to them. They can read the content comfortably and share their ideas in structured ways [177]. Active participation of students in online bulletin boards proved healthy for the students in comparison to passive or non-users [83]. A study was conducted by Yilmaz in 2016 [196] to explore the structural relationships between knowledge sharing behaviors (KSB), academic staff efficacy (ASE) and sense of community (SoC) of university students in e-learning community. The results of the study revealed that the ASE and SoC of the students positively affect their KSB. The participation of students in an online community of practice cannot be measured by just checking the rate at which students and instructor post on the forum [124]. There is a need to design more subtle measures of the effectiveness of asynchronous discussion forums for learning and teaching.

8.4 Research Method

This study is based on the principles of Design Science Research Methodology (DSRM) [75]. In DSRM, an artifact is created with an intention to solve the identified problem. The artifact is then evaluated in light of its implications. In our study, an artifact is created in the form of UnRizkNow forum to understand the behaviors of students towards the knowledge sharing activities. The forum is then

evaluated with the help of the experiment conducted with the students. The UnRizkNow forum was integrated with a first year Bachelor's course on risk management in NTNU. These students are selected as convenience sample [58] as it was convenient to recruit them for the experiment. Students were assigned various risk analysis assignments and invited to share their knowledge as they worked on group assignments. Students were assigned into four groups, and the group membership stayed fixed for the duration of the course. Data collection was partially from the knowledge sharing platform and partially from a self-administered questionnaire.

8.4.1 Participants & Respondents

The participants in this study were the first year Bachelor's students in Information security program in NTNU. The age of the students was between 19 and 28 years. All the participants had basic training in Information security through a 10 credit course 'introduction to information security' before participating in this study. This study was introduced as a part of a Bachelor's course, Risk Management: Methodology and standards (IMT1132). There was a total of 37 registrants, divided into four groups where each group has (9 ± 1) students. Respondents to the survey questionnaire included 19 students from the same Bachelor's course. Students participated in the knowledge sharing tasks through UnRizkNow forum [183] and in the survey that are approved by the universities' Institution Review Board. They completed the questionnaire anonymously and were assured that participation in the survey would not affect their course grade. However, students were recommended to participate in UnRizkNow forum for better learning and better grade on the assignment.

8.4.2 Setting and process

This study was conducted between February 2016 and July 2016. The students of the IMT1132 course were given an assignment on the application of ISO27005 concepts to different scenarios related to the IT department of NTNU in mid-February 2016. The development of UnRizkNow web forum started in February using phpbb3 [144]. Developing UnRizkNow using phpbb3 provided us many advantages, i.e., add interesting features to the forum, create a private room for each group. The UnRizkNow forum is SSL protected, and only the registered members can view the content being shared. The development and testing of the forum ended at the end of March. The students are handed in the complete project plan for implementation of risk assessment for the given scenarios by 4th March. We introduced the UnRizkNow forum to the students on 1st April. Students are told to share information with other students (inter-group and intragroup) for completing the assignment. They could share their experience, ask questions, suggest the answer and share findings with other group members. The objective of this ex-

ercise is to encourage students to share valuable information with each other and help each other to solve the common task effectively. The forum has a 'thanks for posts' feature to allow users to thank the poster for good content. The concept of thanks for the post is derived from [140].

8.4.3 Survey instruments

In this study, an online-based questionnaire was an instrument. The questionnaire was in the Norwegian language (English version is available on 15.1) as it was the official language of the course taught. The questionnaire was designed using the Google form and handed out to the students on 26th May. The questionnaire, consists of 10 questions, was related to students' demographics, ISO/IEC 27005 and project work, use of web forum (UnRizkNow) and data sharing. A Likert scale was chosen to describe 'degree of agreement,' 'intensity of value' for several questions. The degree of agreement was described on a scale from 1 to 6. On this scale, selecting the 1 means that the statement is "Strongly disagree" and the 6 means "strongly agree." So students were asked to indicate how strongly they agreed with the statement on a scale from 1 to 6, with higher numbers indicating a stronger agreement that the statement is true. The intensity of value was defined on the scale of low, medium and high. The authors of this paper designed the questionnaire for the survey. The questionnaire stated in [153], [24], [196] served as the foundation blocks to create the questionnaire for this study.

8.4.4 Data collection and Data analysis

The usage data in the UnRizkNow forum (activity and posts) was gathered in order to provide an overview of students' behavior towards participation in knowledge sharing activity. This task was done through the Admin control panel (ACP) of UnRizkNow forum. The information related to the posts, details of registration, the activity of each member was collected and logged into the excel file.

The data of the questionnaire was collected using the Google form service. The collected data is entered into SPSS Version 23 manually. For the multiple response questions of the questionnaire, data was converted into multiple response data set in SPSS [160]. The data set of the study was examined regarding sample size, normality. The Null hypothesis is that "sample distribution is normal." The data from the scale is examined via the Shapiro-Wilk test in SPSS as the sample size is less than 50. The *sig.* value of the Shapiro-Wilk test is not higher than 0.05 for any data set. Hence, we rejected the null hypothesis and considered our sample data as non-normal [66]. Descriptive statistics (e.g., frequency, percentage, standard deviation) was used in analyzing the data because there is no hypothesis to test in this study. We are mainly interested to see the most critical behaviors among the

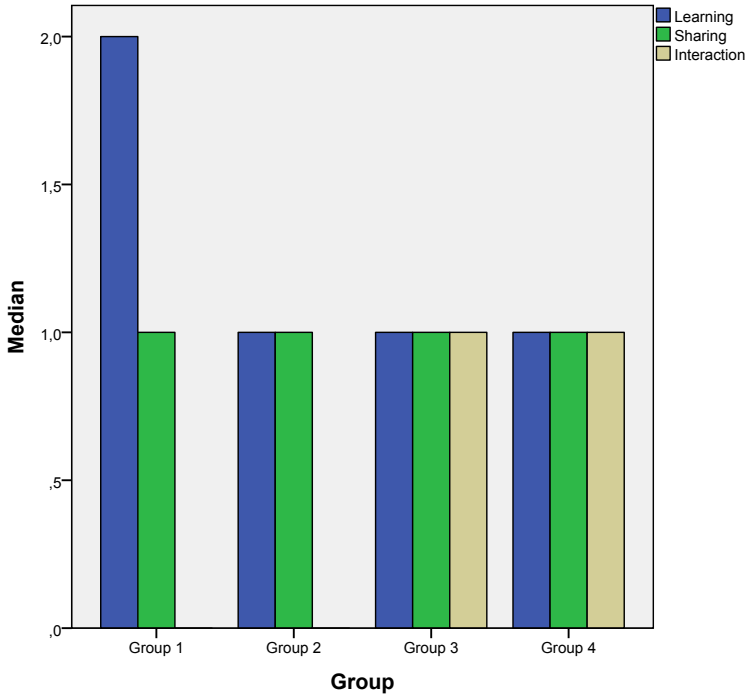


Figure 8.1: Significance of UnRizkNow in the context of learning, sharing contents and interacting with teachers according to participating groups

students in the context of knowledge sharing activities.

8.5 Findings

This section highlights the findings of the data analysis done in this study. Students and the instructor used the forum for 8 weeks (from 1st April to 2nd June 2016). There are 37 posts, 19 topics and 42 users (37 students, 1 teacher, 1 member from the IT department, 1developer, 2 external users) as of 2nd June.

8.5.1 Significance of UnRizkNow in sharing, learning and interacting

We also gathered data on the perception of students for UnRizkNow forum in the context of sharing knowledge, learning new concepts, and interacting with the course instructor through the study. The value of the question was assigned using low, medium, high on the Likert scale.

Figure 8.1 shows the distribution of values among the participating groups. According to Group 1, they found the UnRizkNow forum better for learning than

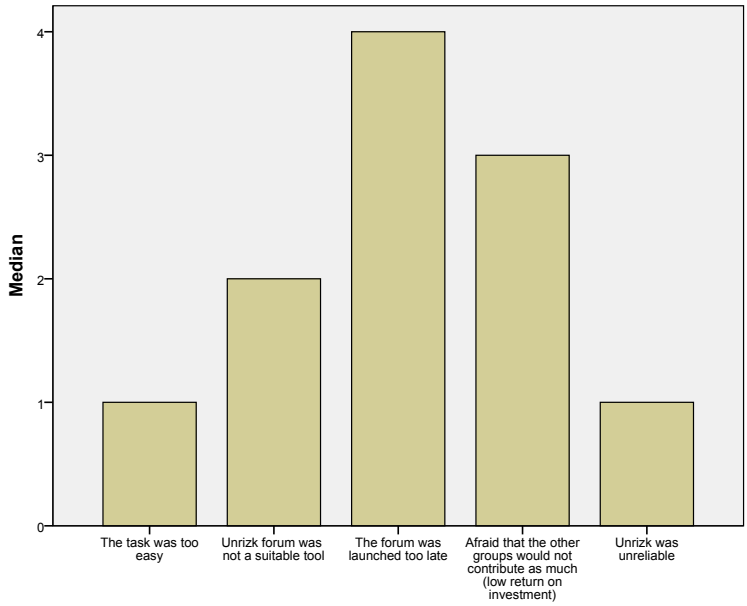


Figure 8.2: Distribution of factors affected the use of UnRizkNow

sharing and interacting. Group 1 is the most active group on UnRizkNow forum. They contributed more than 50% towards the content of the forum. Members of Group 1 used the forum to ask questions related to their assignment to seek answers from the others. We observed in our study that Group 1 used the concepts in their assignment report to solve the task. According to the course instructor, it enhanced the quality of their report.

8.5.2 Factors affecting the use of UnRizkNow

We also observed during the experiment that the traffic is moderate on the UnRizkNow forum. Therefore, we asked the students to indicate the reason through the questionnaire. Figure 8.2 shows the distribution of students' response under five categories. Students responded that UnRizkNow forum was introduced very late to them. Therefore, they had a low motivation to use UnRizkNow extensively. We also categorized this data according to participating groups in Figure 8.3. A high number of members of each group answered that the forum was launched too late (mean value greater or equal to 4) for their assignment. The second factor that demotivated them to use UnRizkNow is the low return on Investment.

We also collected other factors (as a free text from the students through the survey) through comments from the students in the questionnaire. The summary of these

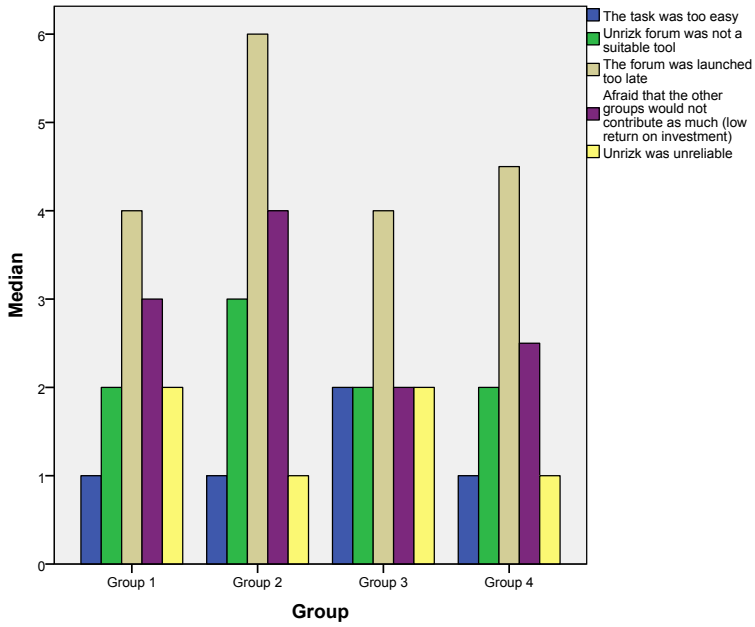


Figure 8.3: A clustered graph to show factors affected use of UnRizkNow in each participating group

findings are a) A few students do not participate in sharing information because they are afraid what they are sharing might be wrong or irrelevant to other group members, b) Students are skeptical of using UnRizkNow as it is a new forum for them. They are more comfortable to use well-known social platform having more participants, e.g., Facebook, c) Students are busy in other activities related to their assignment when they are introduced to UnRizkNow forum, d) Students lost motivation as they can't see others are participating or contributing equally, e) Many students failed to realize the benefit of cooperating with other groups. According to them, cooperation within their group is more important than cooperation with other groups to complete the assignment.

8.5.3 Suggestion to enhance participation and sharing

We collected suggestions from students to enhance various features of UnRizkNow forum that can encourage students' participation and motivate them to share knowledge on the forum. The outcome of this task is particularly beneficial for the future development of the forum. We can understand different incentives that can be of high interest to the students. The findings are: a) Introduce the forum as soon as possible in the course timeline; b) Create a notification system so that inter-

ested/subscribed members receive a notification when something is posted on the related topic; c) Introduce a tag system to structure the information; d) Introduce a competition among the students to increase participation for most useful posts; e) Create a reward system, e.g., monetary, reputation, grade points

8.6 Discussion

The research confirmed that UnRizkNow generated a moderate volume of traffic. Students showed limited motivation towards participation on UnRizkNow and sharing knowledge with others. In the pursuit of explaining the students' behavior and answering our research questions, we explored several theories that deals with attitude, motivation, perceived behavioral control, subjective norms. We categorized these theories into two levels that are explained as follows:

8.6.1 Individual level

Knowledge is highly personal to an individual or a team. Knowledge is *"intimately and inextricably bound with people's egos and occupations [47]."* According to [172], people fail to share knowledge in the absence of any strong personal motivation. Therefore, individuals' willingness to share the knowledge is a crucial factor that must be taken into account in any knowledge sharing activity. *Social exchange theory (SET)* suggests that individuals evaluate the perceived ratio of benefits to costs and plan their actions to maximize their benefits [52]. The benefits can be expressed as money, respect, reputation or any other tangible incentives. In this study, students indicated that they failed to perceive the benefit of cooperating with other groups to share knowledge on the forum. According to the *Theory of Motivation and Barriers* (TMB) [21], people are not always clear on what should be shared with other participants. They hesitate to share out of fear of criticism, or of misleading the community members. They are not sure if the contributions are significant, accurate or relevant to the discussion. This problem is mainly observed in the community of practice having novice or newcomers as participants. Our study confirms this theory. There is also an interesting outcome related to confidentiality and privacy in this study. The students never indicated confidentiality and privacy as a reason for low participation in knowledge sharing activity on UnRizkNow. The possible explanation of this behavior is the presence of a certain degree of *trust* in the working group. Trust within a workgroup refers to the extent to which group members believe that an individual will not intentionally harm another when given the opportunity to do so [122, 113]. The participants in this study had worked together previously as they are students of the same Bachelor's course. This can be the reason for having some degree of trust in sharing information with others. However, the verification of this theory needs further research work.

8.6.2 Community level

At the community level, the presence on the online platform and sense of community play a critical role in influencing students' motivation for participation in online knowledge sharing activity [40]. According to *Social Presence theory (SPT)* [166], the presence of other participants in CoP is important because it enables direct or indirect contact with others. People prefer to communicate with the trusted party, whether face-to-face or by any other means. The perception of the high degree of social presence and having direct or indirect human contact contribute to the building of trust. Extending this logic to the setting of CoP, the trust may be built by establishing the feeling of high social presence. UnRizkNow is a relatively new forum with a few users (only 42 users altogether) to participate in the knowledge sharing task. Hence, UnRizkNow lacked in establishing a sense of social presence on the forum. Research has found that richer media (media with higher social presence) tend to be preferred in communication settings where the task is ambiguous and uncertain [173]. According to the *theory of planned behavior (TPB)* [16], more favorable attitudes toward a specific act, more favorable subjective norms, and greater perceived behavioral control strengthen the intention to perform the behavior. In the settings of this study, it seems that the more the students are aware of the online presence of fellow participants, the more likely they will be engaged in the activities of the community. This theory also suggests an interesting fact that participants are not only the contributors of information but also creators of a context to provide momentum to an online community [49]. In this study, we observed a clear effect of the theory of planned behavior among the students. Students mentioned in the survey that they lost motivation in knowledge sharing task because they could not see other participants contributing equally.

8.7 Research limitations and Future work

The data collection is restricted to the students of a Bachelor's program in NTNU. Due to a rather small sample size of the students in the study and their unique background of being in an education course, the findings may also not be immediately generalizable to other contexts. Hence, more studies are needed to generalize present study findings. In order to verify and generalize the research results, the research should be expanded to Information security students of different expertise level. We had limited control over the course activities, and requirements. Therefore, we could not introduce different incentive schemes (e.g., reward, grade, score) during the course activities. It would be an interesting exercise to observe any correlation between the behaviors of students and incentive schemes. Most of the students had already set up their tasks on other social platforms as UnRizkNow was introduced a bit late to the students. We believe that the introduction

of UnRizkNow in the earlier phase would generate a slightly different outcome. However, the verification of this assumption needs further experiments. The next version of UnRizkNow will include some new features (incentive schemes, better communication features, a large reservoir of study materials) that may encourage practitioners to participate in the study. Our long-term goal is to launch UnRizkNow for the CSRM practitioners in small and medium-sized enterprises. Therefore, the focus of our future studies is to include CSRM practitioners to carry out research activity.

8.8 Conclusion

The objective of this study is to explain the behaviors of students towards knowledge sharing activities on UnRizkNow forum. An artifact is designed and developed in the form of UnRizkNow forum. In order to evaluate the developed artifact, an experiment is conducted with a small set of Information security students to observe their behaviors. Later, responses are collected from the same participants to understand their perception of this activity. We observed mild traffic on UnRizkNow during the experiment. The activity of knowledge sharing is not significant in the forum. The study confirms that Theory of Motivation and Barriers (TMB) has a strong influence on the behavior of students as a large number of students are not sure what they should share and the relevance, correctness of the content that they share. They are also afraid of wasting their effort and time on knowledge sharing activity when other members are not participating equally. The social exchange theory (SET) successfully captures this behavior as students perceived the ratio of benefits to costs low in this activity. We are interested in studying the behaviors of a large population working in the area of CSRM. Our future research will be directed to achieve this goal.

8.9 Acknowledgment

This study is a part of UnRizkNow project, which is funded by CCIS. Gaute Wangen helped us to introduce UnRizkNow forum to his Bachelor's students, write content for the forum, and translating questionnaire contents to the Norwegian language. We would like to thank the students of IMT1132 for their participation in this study, and anonymous reviewers for their comments.

Chapter 9

Article 2: CIRA perspective on risks within UnRizkNow - a case study

Vivek Agrawal & Adam Szekeres, CIRA perspective on risks within UnRizkNow - a case study, IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 121-126

9.1 Abstract

UnRizkNow is a community of practice for cyber security practitioners in Norway. It is imperative for the establishment of UnRizkNow to identify the underlying risks that can affect the normal operation of the community. This paper presents a study to carry out a risk assessment of UnRizkNow CoP using conflicting incentive risk analysis (CIRA) method. The main contribution of this research work is to identify and analyze the risks that can be obtained from the conflicts in the incentives of members and organizer in UnRizkNow. This paper also presents a risk treatment plan in terms of incentives as suggested by CIRA method. The findings of this study are helpful to establish UnRizkNow community, and also for the researchers who want to analyze human risks in a system.

9.2 Introduction

Sharing and re-use of information improve both quality and cost effectiveness of the knowledge sharing activities. Therefore, communities of practice (CoPs) is gaining popularity among the professional practitioners recently. The focus of

learning is strongly shifting towards online community-based modes of training in organizations [49]. Learning within a community is concerned with participation in the activities of creating, sharing and construction of knowledge. The learning that evolves from these communities is collaborative in nature, i.e., the collaborative knowledge of the community is greater than any individual knowledge [115]. However, many CoPs have failed because the community stakeholders had either insufficient idea about the benefits/incentives of being involved in such communities or the incentives perceived by them are conflicting in nature.

UnRizkNow is being formed as a community of practice (CoP) for the information security risk practitioners in Norway. UnRizkNow can play a key role in the promotion of learning and innovation in the field of cybersecurity risk in contemporary organizations. However, establishing and sustaining UnRizkNow is not a trivial task. There will be several stakeholders involved in the various activities associated with a CoP. The action of the stakeholders is often motivated by the incentives/ benefits perceived by them [151]. It may give rise to complex risks which are impractical to be expressed as a combination of likelihood (probability) and consequence. It is also difficult to obtain historical data to validate probability associated with the calculation of risk in the system. Conflicting incentives risk analysis (CIRA) specifies risks in terms of conflicting incentives between the stakeholders. CIRA considers human factors in order to analyze risk in a system. Therefore, CIRA is a good candidate to assess underlying risks in UnRizkNow. We are particularly interested in answering the following research questions (RQ) in this study:

RQ1 What are the incentives of the *members* and the *organizers* of UnRizkNow community?

RQ2 To what extent can CIRA uncover the risks generated from conflicting incentives in UnRizkNow?

RQ3 What are the risk mitigation plans that can be designed using the concepts of CIRA method?

The main contributions of the work are: a) Explain the features of UnRizkNow CoP; its stakeholders and their incentives - Answers RQ1, b) Apply conflicting incentive risk analysis (CIRA) method to UnRizkNow to investigate the underlying risks - Answers RQ1, c) Identify risk scenarios that can be generated in UnRizkNow due to the conflict between the stakeholders - Answers RQ2, d) Suggest risk mitigation plans for the risk scenarios identified for UnRizkNow - Answers RQ3

9.3 Background Knowledge

This section provides an overview of the community of practice and CIRA method. The main features and objectives of a CoP are described along with the information on the necessary steps of CIRA method.

9.3.1 Community of practice (CoP)

The term 'communities of practice' [192] is fairly a new term to denote community-based learning method. However, the phenomenon referred by CoPs has very old existence. CoP [192] is a common way to engage people in sharing knowledge, discuss issues, and learn from others' experience to resolve several challenges in many organizations. Wenger provides the theoretical basis of communities of practice in [192]. According to Wenger, "'Communities of practice are groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly."' The cop is well-suited for the development and sharing of knowledge and practices across divisions. A CoP mainly consists of three fundamental elements [192], [195]: A *domain* of knowledge creates common ground, inspires members to participate, guides their learning and gives meaning to their actions; The notion of a *community* creates the social fabric for that learning. A strong community fosters interactions and encourages a willingness to share ideas. While the domain provides the general area of interest for the community, the *practice* is the specific focus around which the community develops, shares and maintains its core of knowledge. Members of CoPs learn from each other in the community and deepen their knowledge and expertise. Members of the CoPs are often termed as *practitioners* as they learn from peers through practice [26]. Communities mainly consist of people (stakeholders) who have some incentive to be a part of a given community of practice.

9.3.2 Conflicting Incentives Risk Analysis

Conflicting Incentives Risk Analysis (CIRA) is a risk analysis method which is developed by Rajbhandari and Snekkenes [151]. This method is based on the idea of qualitative analysis. This risk can be intentional as well as unintentional. CIRA method identifies stakeholders, actions and perceived expected consequences that characterize the risk situation. In CIRA, a stakeholder is an individual that has some interest in the outcome of actions that are taking place within the scope of the significance. There are two classes of stakeholders: the strategy owner and the risk owner. Strategy owner is the stakeholder who is capable of triggering an action to increase his perceived benefit. The stakeholder, whose perspective is considered when performing the risk analysis, is a risk owner. Typically, each stakeholder has associated a collection of actions that he owns. CIRA focuses on

the human-related risks which correspond to understanding the incentives of the stakeholders that influence their actions. An incentive motivates a stakeholder to take action to increase his expected/ predicted utility. The utility is the benefit as perceived by the corresponding stakeholder and it comprises of utility factors [10].

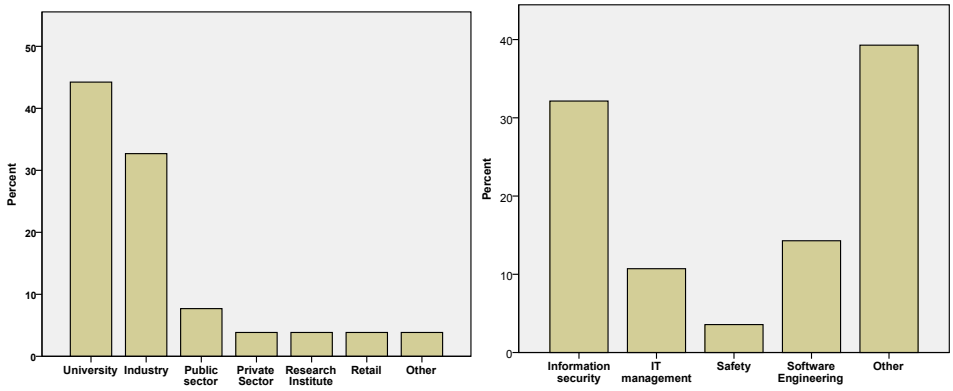
9.4 Related work

The basic concept of a community of practice is presented by Lave & Wanger [109], and by Brown & Duguid [31] in 1991. However, both the works could not provide a clear definition of a community of practice until Wenger [191] provided one in 1998. The significance of CoPs in terms of fostering knowledge management, exchange of expertise and information, collaboration within organizations has been described in [60], [126]. Wenger [192] mentioned that building trust among the members, sharing ideas across different organizational units, and respecting different national and international cultures of the members in a community are the biggest obstacle in establishing a distributed community of practice. There are several other challenges identified for establishing and sustaining COPs within organizations [176]. For instance, Bourhis et al. [30] believed that finding common interesting topics for the members is the biggest challenge in a CoP; lowering barriers among the members to overcome 'information hoarding' problem [21]; recruiting the right members (experts, practitioners of the given domain) who have sufficient knowledge and enough time for social interaction [142]. Probst et al. [148] presented a study to highlight possible reasons behind the success and failure of communities of practice. They investigated 57 CoPs from major European and US companies. The survey revealed that weak one-to-one connections between the members, rigidity of competences, lack of identification in the network, practice intangibility are the main reasons for the failure. Conflicting incentive risk analysis (CIRA) is applied to a few cases to evaluate the human-centered risks [151], [152]. The application of CIRA to a more complex incentive system is done in the study [188]. The studies conducted using CIRA method are serving as a good starting point for this study. A pilot study is done with UnRizkNow to investigate the knowledge sharing behaviors of the students (members) on the community of practice [12]. The study examined the behaviors of the students and explained it using descriptive theories.

9.5 Research Methodology

9.5.1 Survey instrument

An online quantitative questionnaire was created using LimeSurvey. The survey was hosted on our project domain [7]. The survey comprised of 17 questions (39 questions including sub-questions) in total that assessed various aspects of inform-



(a) (b)

Figure 9.1: Details of the respondents: (a) Affiliation (b) Domain

ation sharing and previous experiences with CoPs. The survey was distributed online through several channels, see Table 9.1. The survey was added to the official monthly mailing list of NorSIS, distributed to the members of NisLab through intranet and email. The questionnaire was available in both English and Norwegian languages. 7-point numerical rating scales were used (1-Not at all, 7-Extremely) for evaluative questions, and lists of possible answers were provided for categorical questions.

9.5.2 Respondents

A total of 52 respondents (43 males, 8 females, 1 undisclosed) volunteered to *complete* all the sections of the online survey. The majority of the respondents were between the ages of 25-34 years (34.6%). The majority (about 76.9%) of the respondents are affiliated with the university and industry (see Figure 9.1a). However, the survey did not include students as potential respondents as we are interested in getting the opinion of the professionals for this study.

9.5.3 Data collection and data analysis

Data for this study is collected through an online survey, and literature study. The list of the stakeholders for a community of practice is designed using the literature [106], [132]. The incentives of the stakeholders are chosen based on the responses collected from the survey [7]. The survey was conducted in three phases between 28.11.2016 and 10.01.2016. The details of each phase in terms of duration, the medium through which the survey was distributed, no. of respondents, and the number of complete responses are given in Table 9.1.

Table 9.1: Details of the data collection activity

Phase	Duration	Medium	Respondent
Phase1	28.11.2016-06.12.2016	NorSIS	13
Phase2	19.12.2016-10.01.2017	NISLab	19
Phase3	30.11.2016-19.12.2016	Email	17
		LinkedIn	3
Total	**28.11.2016-10.01.2017**	**Online**	**52**

We used IBM SPSS statistics 24 (NTNU licensed) to analyze the survey data. Out of 52 respondents, 28 respondents have already participated in a CoP, whereas 22 members answered that they want to join a CoP. 2 respondents neither participated in any CoP, nor they want to participate. The domain of the CoP that the people participated in is given in Figure 9.1b.

Respondents have indicated their roles in the CoP that they participated in and also the role that they want to take in the future CoPs, Table 9.2. The majority of the respondents are interested in participating in a community as a 'member'.

Table 9.2: Distribution of the roles in CoP

Role in the community	Sponsor	Organizer	Member	Facilitator	Leader
Votes	2	5	43	5	3

The data set of the study is examined in terms of sample size, normality. The Null hypothesis is that "sample distribution is normal." The data from the scale is examined via Shapiro-Wilk test in SPSS. The sig. value of the Shapiro-Wilk test is not higher than 0.05 for any data set. Hence, we rejected the null hypothesis and considered our sample data as non-normal. We used median or mode in order to compare the response, and assign a weight for the survey questions that involve answers on the numerical rating scale (1= Not at all, 7= Extremely). The mathematical model in our survey design assumes that the interval between values is not interpretable (i.e., the distance between 1-2 is not the same as the distance between 6-7). Therefore, calculating the mean or standard deviation on the given data is not a suitable approach to build any conclusion.

9.6 Case study

This section presents a case study of UnRizkNow community of practice using the CIRA method. The objective of this section is to answer the research questions, RQ1 and RQ2. Firstly, an overview of UnRizkNow community is provided with an emphasis on the involved stakeholders, their roles, and incentives. Secondly, CIRA method is applied to UnRizkNow to find out the conflict in the incentives and potential risks it may cause.

9.6.1 Overview of UnRizkNow

UnRizkNow [184] is an Online Cyber Security Risk Management Community of Practice (CoP) for Cyber Security Risk Management (CSRM) practitioners in Norway. The objective of UnRizkNow is to identify relevant challenges that CSRM practitioners face in their field of interest and enable them to resolve these challenges by sharing knowledge in the form of ideas, answers, and experience. The *domain* of UnRizkNow is the area of shared expertise and key issues in the field of information security management. The *community* consists of the Information Security practitioners working in small and mid-sized enterprises. The practitioners must be committed to a process of collective learning oriented toward achieving outcomes and improving practice. The members will *practice* the investigation of key questions, problems, and challenges faced by the practitioners; identification of resources and expertise, improving the subject knowledge through learning, and development of new processes, methods, and knowledge.

9.6.2 Analysis of UnRizkNow using CIRA

The following section describes the steps for conducting a risk analysis of UnRizkNow according to the CIRA method [151]. For the present case study the possible misalignment of incentives between the community *Members* and the *Organizer* is investigated. The analysis focuses on the general description of possible risk situations in a CoP context and employs a qualitative analysis similar to the one presented in [188].

Step 1. - Identify the risk owner: A community member is considered to be the risk owner.

Step 2. - Identify the risk owner's key utility factors: Based on the survey responses, four aspects of information sharing were considered as key utility factors for the risk owner. The selection was made by calculating the statistical mode for each of the presented factors, and one was selected from each differentiating categories. The key utility factors are as follows:

Improve knowledge: the motivation to gain a better understanding about the do-

main knowledge, make use of the information shared by community members.

Share experience to help others: refers to the intrinsic value of sharing valuable experiences for the benefit of others.

Handling of privacy and confidentiality: trust in the community and all stakeholders that the shared professional/private information is used confidentially and according to relevant privacy agreements.

Building reputation: refers to the esteem, recognition received from others in the community, achieved by presenting relevant skills and competence in the domain.

Table 9.3: A strategy's effect on the Utility Factors relative to their assigned weights

		Effect on Utility Factors		
Statistical mode derived from survey	**Weights**	**Increase**	**Unaffected**	**Decrease**
7	**Very High**	+5	0	-5
5-6	**High**	+4	0	-4
4	**Medium**	+3	0	-3
2-3	**Low**	+2	0	-2
1	**Very Low**	+1	0	-1

Step 3. - Given an intuition of the scope/system identify the kind/ classes of operations/ strategies which can potentially influence the above utility factors: The standard CIRA method distinguishes between *threat risks* and *opportunity risks* - the risk when the strategy owner is not motivated to take an action that would be beneficial for the risk owner [150]. However, we restricted the analysis to risks that are potentially harmful to the risk owner. The following strategies were identified as being capable of having a negative impact on the aforementioned utility factors: *Misuse of the community knowledge/information:* using the useful information shared by the members of the community for another purpose than that is mentioned in the policy without receiving consent or the disclosure of any secret information of the community members to unauthorized parties; *Diverting the purpose:* changing the topic or purpose of the community from the one that was told to the members while recruiting; *Selection of inappropriate members:* recruiting the irrelevant/unsuitable members for the community mainly for the purpose of projecting high presence of the members on the community and earning

money in the form of membership fee. A person who is associated with other such community of practice is not allowed to join the community; *Improper incentive scheme:* overlooking the preferences of the community members when designing an incentive system, leading to unintended consequences or dissatisfaction [106].

Step 4. - Identify the roles/functions that may have the opportunities and capabilities to perform these operations: Even though various stakeholders might be able to implement some of the strategies as mentioned above, in the present case study the Organizer is considered to be the strategy owner.

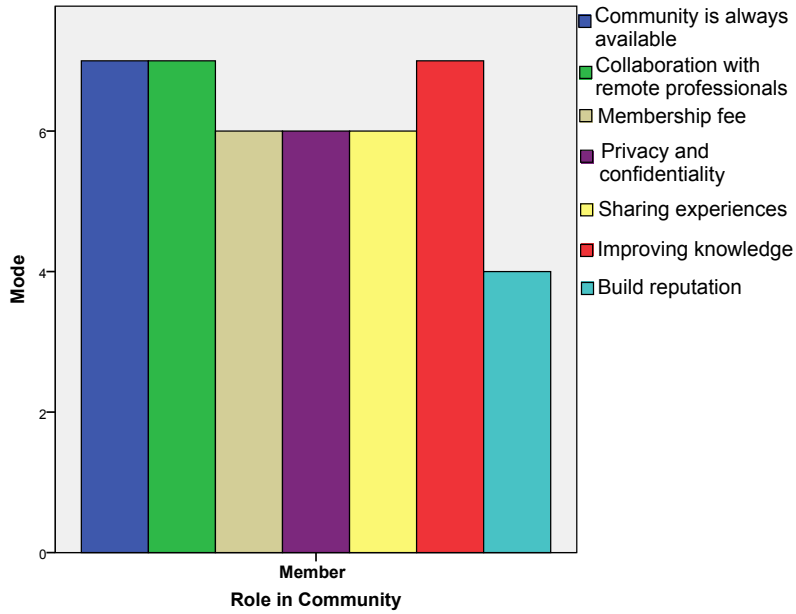


Figure 9.2: Statistical mode for each aspect of information sharing investigated

Step 5. - Identify the named strategy owner(s) that can take on this role: This step is excluded from the present analysis. Since UnRizkNow is in a pre-deployment phase, this role is not yet fulfilled by any individual.

Step 6. - Identify the utility factors of interest to this strategy owner(s): The following utility factors are considered to be relevant for the Organizer in the CoP setting: **Revenue:** Can be generated by collecting membership fees from members. A decision has to be made between increasing the number of members or setting a higher membership fee. Promoting the community among the professionals, securing money from the sponsors. By selling the knowledge/technology

designed in the community to third parties. **Reputation:** The Organizer is interested in establishing a good reputation in the business community.

Step 7. 8. 9. - Determine how the utility factors can be operationalized, how each of the stakeholders weights the utility factors, and how various operations result in changes to the utility factors for each of the stakeholders: - A deviation from the standard CIRA procedure is that the identified utility factors are investigated qualitatively that allows discovering general risk scenarios that might emerge in Communities of Practice, whereas the standard procedure focuses on individual differences between the stakeholder's perception of benefit. The investigation here aims to describe reasonable situations that might pose a threat to the risk owner, not to analyze whether a given risk will manifest itself. Therefore, the operationalization of the utility factors is excluded from the present analysis. The mapping between the weights assigned to the utility factors and the direction of influence by any strategy is presented in Table 9.3. The results from the survey served as input for defining the weights for the selected utility factors. Figure 9.2 shows the statistical mode for each aspect of information sharing. The selection was made such that they represent different levels of importance for the community members. Table 9.4 illustrates the utility factors and their corresponding weights for both of the stakeholders, the four strategies identified as being capable of influencing these utility factors and their effect taking into account the utility factor's importance.

Table 9.4: Overview of the incentives in relation to various strategies

			Influence of strategies on Utility Factors			
Stakeholders	**Utility Factors**	**Weights**	Misuse of the knowledge / information	Diverting the purpose	Selection of inappropriate members	Improper incentive scheme
Member	Improve knowledge	Very High	Unaffected (0)	**Decrease (-5)**	**Decrease (-5)**	Unaffected (0)
	Share experience to help others	High	Unaffected (0)	Unaffected (0)	**Decrease (-4)**	**Decrease (-4)**
	Confidentiality and privacy	High	**Decrease (-4)**	Unaffected (0)	Unaffected (0)	Unaffected (0)
	Build reputation	Medium	Unaffected (0)	Unaffected (0)	Unaffected (0)	Unaffected (0)
Change in utility			**-4**	**-5**	**-9**	**-4**
Organizer	Revenue	Very High	**Increase (+5)**	**Increase (+5)**	**Increase (+5)**	Unaffected (0)
	Reputation/ user satisfaction	Medium	**Decrease (-3)**	Unaffected (0)	**Decrease (-3)**	**Decrease (-3)**
Change in utility			**+2**	**+5**	**+2**	**-3**

Step 10. 11. - Estimate the utility, compute the incentives: As the operationalization of the utility factors was excluded from the analysis, estimating the utility is also omitted. However, it is possible to compute the incentives by investigating whether each strategy has the potential to cause an overall increase, decrease or no change in the sum of the weighted utility factors. The incentive is the potential loss/ benefit perceived by each stakeholder when a certain strategy is triggered. A strategy with a negative incentive is likely to be avoided by the strategy owner, as it lowers his overall utility, while positive incentive suggests actions that are more likely to be triggered.

Step 12. - Determine risk: Risk is considered to be the result of the misalignment of the incentives between the strategy owner and the risk owner. When the strategy owner is in a position to increase his utility while decreasing the risk owner's utility the latter stakeholder faces a risk. Each strategy can be analyzed by comparing the related incentives in order to estimate which action is more likely to take place, i.e., what plans should be developed given the possible outcomes. The risk related to each strategy can be described as a number pair representing the magnitude of undesirability from the risk owner's perspective and desirability (e.g., the strength of the force that motivates the strategy owner) to trigger the corresponding action. In case of the *"Misuse of knowledge/information"* scenario the value is (-4, +2), for *"Diverting the purpose"* scenario (-5, +5), for *"Selection of inappropriate members"* (-9, +2), and for *"Improper incentive scheme"* (-4, -3). Scenarios 1-3 share the common characteristic that they all, to a different degree , can cause a potential loss for the community Member, while increasing the benefit of the Organizer. The fourth option is likely to result in avoidance by each stakeholder, as it would result in loss of utility for both parties.

Step 13. - Evaluate risk: This step refers to the identification of risk acceptance and rejection criteria by the risk owner, as he has to determine whether the identified risks are acceptable or not. This step is not part of the present study due to the lack of named risk owner.

9.7 Discussion

9.7.1 Risk scenarios

The analysis highlighted how various operations influence the overall utility of both Members and Organizer of a Community of Practice. For the present case study, only the Organizer is assumed to possess the capabilities to exert influence on the risk owner and his actions are determined by the desirability attached to each scenario. *Diverting the purpose of the community* is the only strategy that provides a clear and maximum benefit for the Organizer. This strategy might be

implemented when the Organizer chooses to widen the scope of the community in order to increase the number of active participants. The consequence of this strategy is that existing members could find it difficult to gather valuable knowledge from the community since a large amount of irrelevant information could easily reach unmanageable levels.

While both strategies (e.g., *Misuse of the knowledge/ information* & *Selection of inappropriate members*) provide an overall increase in benefit, they represent a more complicated situation where certain trade-off decisions have to be taken into account (i.e., the increase of a potential benefit decreases benefit according to another utility factor). For example, the inclusion of an additional utility factor - representing the contingency of a lawsuit in case of a privacy breach - could provide a more detailed picture of the decisions that the strategy owner might consider. From the perspective of the Members, the worst-case scenario is the *Selection of inappropriate members* as it would create the highest amount of loss interfering with the basic foundations of a CoP at the same time (e.g., community and domain).

9.7.2 Mitigation plans

In the context of CIRA, risk mitigation amounts to modifying the weights that the stakeholders assign to the relevant utility factors or to what extent actions modify the values of the utility factors [167]. For the identified risk scenarios different mitigation strategies can be utilized, addressing RQ 3. The risk experienced by the Member when the Organizer is tempted to play either *"Misuse of knowledge/information"* or *"Selection of inappropriate members"* strategies can be mitigated by identifying other possibilities for revenue generation or by increasing the importance of the other relevant utility factor (Reputation / user satisfaction). Focusing on long-term benefits as opposed to short-term gains might be useful, as it builds on the motivation to create a sustainable community that is a well-known and reliable source of information within the domain. In the case of *"Diverting the purpose"* strategy there are no other utility factors influenced on the strategy owner's side. Therefore, it is not possible to increase the weight of another utility factor. The risk could be mitigated by the introduction of an external regulator (e.g., Sponsor) being responsible for ensuring that the community is kept focused on the selected domain. In the case of the fourth identified scenario, there is no need for risk mitigation as the stakeholders would be in agreement that this situation has to be avoided. Therefore the Organizer can be expected to pay special attention to the development of a proper incentive scheme.

9.8 Research Limitations and future work

The response that we received from 52 participants surely provided initial insight into understanding their preference with respect to the participation in a community of practice. However, the findings cannot be generalized to a large population because of the small sample size of the respondents. The choice of a numerical rating scale (1-7) to collect response also gave us very limited options to compare the utility preferences and weigh them. We cannot calculate mean on a numerical rating scale as it is an ordinal scale. Therefore, we calculated the median and mode to compare the responses for a given question. Calculating median or mode can provide only 7 (for the scale of 1-7) possible outcomes, and it is not sufficient to rank the responses. The application of CIRA method to UnRizkNow is limited to only two stakeholders, i.e., member and organizer in this study. The list of strategies was not intended to be exhaustive, and the primary purpose was to illustrate reasonable actions that are potentially undesirable for the community Members. Therefore, it would be necessary to extend the list to include a wider collection of possible actions that might be suitable for UnRizkNow community. For instance, this analysis did not include actions with direct impact on the Member's *Build reputation* utility factor. In practice, the risk scenarios are more complex as the utilities and strategies of all the stakeholders in the system should be taken into account. The next phase of the study will focus on a more robust data collection approach with a focus to increase the sample size. A series of interviews will be conducted with the prospective users of UnRizkNow to understand their preferences and motivation to participate and share knowledge with others. The responses will help to design sharing rules and incentive scheme for the participants. Afterward, an online platform will be launched as a working prototype of UnRizkNow and users will be invited to join and participate. This task will aim to validate the designed sharing rules, incentive schemes, and effectiveness of UnRizkNow community in sharing knowledge and solving problems of the users.

9.9 Acknowledgment

This study is a part of UnRizkNow project which is partially funded by CCIS. Martin Stokkenes and Gaute Wangen helped us to translate the online survey to the Norwegian Language. Jens Barland provided his input on the dissemination of the survey. NorSIS supported our research work by distributing the survey to the people in Norway. We would like to thank Prof. Einar Arthur Snekkenes for his suggestions on calculating utility factors and risk in CIRA steps.

Chapter 10

Article 3: Factors affecting the willingness to share knowledge in the communities of practice

Vivek Agrawal & Einar Arthur Snekkenes, Factors Affecting the Willingness to Share Knowledge in the Communities of Practice. 23rd International Conference on Collaboration and Technology, CRIWG 2017, Saskatoon, SK, Canada, pp. 32-39

10.1 Abstract

The purpose of this study is to investigate various factors that can affect the willingness of the IT professionals in Norway to share their knowledge in the open communities of practice. The study is conducted through an online survey among the IT professionals working in Norway. The findings of the study present various factors that increase or decrease the willingness to share knowledge on open communities of practice. These factors are further explained with the help of the descriptive theories. The findings of this study are useful to get the initial insight into the determinants that influence the willingness to share knowledge on the communities of practice.

10.2 Introduction

The IT professionals working in different organizations in Norway often face many of the same problems and design similar solutions. The IT professionals also collect and apply the same knowledge to design their solutions. However, it is ineffi-

cient if they do it so mainly on their [57]. Therefore, proper sharing and reuse of knowledge among the IT professionals can improve the quality of their work [185]. We believe that open communities of practice (CoP) [192] can help to achieve the IT professionals in Norway to an optimal level of knowledge sharing. Therefore, we explore the significance of communities of practice for the IT professionals in Norway in this study. There is a lack of studies on the willingness of the IT professionals in Norway to sharing knowledge on open communities of practice. The prospective members from the industry and academia in Norway are invited to participate in an online survey to state their preference regarding the sharing of knowledge on CoP. We collected the response of the participants for six weeks. Our study provides insight into the factors that can increase or decrease one's willingness to share knowledge in communities of practice. We believe that these insights are essential to improve the current state of knowledge sharing. We are particularly interested in answering the following research question in this study:

RQ1 What are the factors that influence the willingness of the professionals working in Norway to share their knowledge in the open communities of practice?

The CoP is a common way to engage professionals in sharing knowledge, discuss issues, and learn from others' experience to resolve several challenges in many organizations. CoP often focus on sharing best practices and creating new knowledge to advance a domain of professional practice. However, the community members often tend to hide the information or not share with others if they perceive that the knowledge they possess is valuable and important [21]. Therefore, it is imperative to determine the factors that act as a motivation or barrier for the IT professionals to share knowledge with others in a community-based information sharing arena. This study contributes to our understanding of the motivation and barriers that IT professionals in Norway face in sharing knowledge on the *open* CoP. CoP that exist as a *closed internal* or *joint venture* are not considered as a part of this study. We are more interested in learning about the preferences of the members towards the CoP where the membership is not dependent on the member's affiliation. In this study, knowledge refers to all professional information, i.e., income, affiliation, ability to learn a concept, critical thinking, problem-solving ability.

10.3 Related work

The term 'communities of practice' is a relatively new term in the area of knowing and learning, but the phenomenon it refers to has a very old existence [192]. According to Wenger [191], *"'Communities of practice are groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly."'* Knowledge sharing is a process that exploits existing knowledge by identifying, transferring and applying to solve tasks better, faster

and cheaper [81]. Knowledge sharing is essential for the innovation in organization and the individual. Cabrera et al. [33] presented several difficulties that an organization faces in encouraging its employees to share knowledge with co-employees and presented several knowledge-sharing dilemmas. Ardichvili et al. [21] conducted a qualitative study to investigate the motivation and barriers to employee participation in online communities of practice at Caterpillar Inc. This study revealed that the members of the community are skeptical towards knowledge sharing because of the fear of criticism or misleading others. There are several studies [64], [154] that explored the role of trust in the context of online professional communities. Gagné [63] presented a model of knowledge-sharing motivation based on a combination of the theory of planned behavior (TPB) and self-determination theory (SDT). He argues that more positive attitudes toward knowledge sharing can be achieved out of interest or personal meaning. The influence of culture on the knowledge sharing strategies in online CoP is studied in [22].

10.4 Research method

In this study, the determinants, which increase and decrease the willingness to share knowledge on CoP, are drawn by the response stated by the respondents. An online survey-based technique is designed to collect the preference of the professionals working in IT-industry in Norway.

A free open source software survey tool, LimeSurvey, was chosen to create an online quantitative questionnaire survey. The survey was hosted on our project domain. The survey comprised of 39 questions [1] in total that assessed various aspects of information sharing and previous experiences with CoPs (see Appendix 15.2). The survey was distributed online through several media from 28.11.2016 to 10.01.2017. The online survey was available in both English and Norwegian. Seven-point Likert-type scales ranging from '1' (Not at all) to '7' (Extremely) were used throughout the questionnaire. The idea of using a Likert-type scale to conduct this survey is derived from the work of [175], and the range of scale (1-7) is selected based on the argument given in [18].

A total of 52 respondents (43 males, 8 females, 1 undisclosed) volunteered to complete all the sections of the online survey. The majority of the respondents were between the ages of 25-34 years (34.6%). The majority (about 76.9%) of the participants are affiliated with a university and industry. However, the survey does not include student as a potential participant as we are interested in getting the opinion of the professionals for this study.

We used IBM SPSS Statistics 24 (licensed) to analyze the survey response. We

[1] survey link: https://www.unrizk.org/survey/index.php/346746?lang=en

Table 10.1: Participation of respondents on different types of CoP

Nature of the community	**Percent**
Both online and offline	43
Offline	11
Online	43
Other	4

used median or mode to compare the response, and assign a weight for the survey questions that involve answers on the numerical rating scale (1= Not at all, 7= Extremely). The mathematical model in our survey design assumes that the interval between values is not interpretable (i.e., the distance between 1-2 is not the same as the distance between 6-7). Therefore, calculating the mean or standard deviation of the given data is not a suitable approach to building any conclusion.

10.5 Research findings

In this section, the result of survey response is presented to get an insight into the research questions.

10.5.1 Participation in CoP

Out of 52 respondents, 28 respondents have already participated in CoP. The other 22 members stated that they want to join a CoP. The remaining two respondents neither participated nor they want to participate in any CoP. Among the 28 respondents who have participated in a CoP previously, 43% have participated in the online CoP (web portal, online forum), whereas only 11% have taken part in the offline CoP in the form of face to face discussion.

Table 10.1 gives the information that there are a few respondents who have participated in both online and offline form in the community.

The respondents, who stated that they have participated (n=28) in a community of practice before, were asked to state the domain of the community.

Table 10.2 displays that most of the respondents (33%) have participated in Information security community, 15% of the respondents have participated in the software engineering community. The respondents have also mentioned the communities that were not given in the questionnaire options. For instance, knowledge formation in the organization, building rules and regulation of the organization.

Table 10.2: Domains of the community where the respondents participated

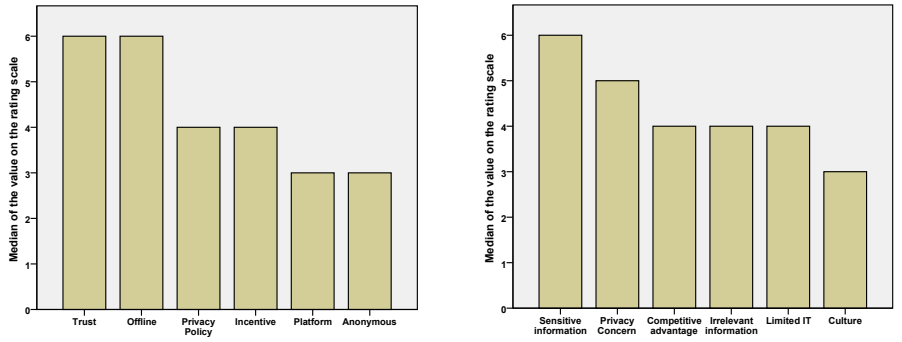
Domain of the CoP	Percent
Information Security	33
Other	26
Software Engineering	14
IT management	12
Web development	6
Safety	3
Online marketing	3
Journalism	3

10.5.2 Factors increase willingness to share knowledge

Respondents were asked to rate different factors that increase their willingness to share knowledge with others on the scale of 1-7 (Likert scale). Figure 10.1a displays the graph representing the distribution of the median of various factors. Respondents stated that having trust with the receiver of the information, and meeting the person face to face are the most important factors that increase their willingness to share knowledge. The presence of a privacy policy that includes the detail about how the shared knowledge can be treated and used is also essential for the participants. The respondents also stated that an incentive (Useful knowledge, money, fame, reward) is necessary to encourage them to share knowledge. Having an incentive system gives them a better perspective of high return on investment, where the investment is an apparent effort, time, and giving out knowledge. According to our study, anonymity and the presence of online platform do not contribute much toward increasing the willingness to share knowledge.

10.5.3 Barriers to share information

Figure 10.1b shows the median distribution of different factors that act as a barrier to sharing knowledge in the community. The higher the value on the median scale the stronger the given factor serves as a barrier to sharing knowledge. The most significant barrier that was stated by the respondent is the breach of confidentiality. The participants of the community may share something that is very useful for the receivers, but at the same time can contain some sensitive information. The leakage of the confidential/ sensitive information can harm the individual. The second most significant barrier is the concern of privacy breach by participating in the knowledge sharing task in the community. A few respondents indicated that they do not share information if they feel that they will lose the competitive advantage by sharing it. The concern of receiving irrelevant information from the



(a) (b)

Figure 10.1: a)Motivation b) Barriers

others also lower down the willingness to share something useful with others. The presence of limited IT resources is also a significant barrier for a few respondents. The respondents have indicated the effect of culture as a barrier as very low.

10.6 Discussion

The main objective of the present study was to identify and understand the determinants of knowledge sharing task on communities of practice. The survey results indicate the influence of social exchange theory (SET); people are concerned about the absence of any benefits to share knowledge. People tend to share the knowledge they possess with others when they feel that they will also receive quality information from others. However, the tendency to share knowledge decreases when it is perceived that they are receiving irrelevant or not so useful information from other members. In this study, respondents indicated that from their experience, the communities did not score well in providing meaningful incentives to the members. Therefore, it is important for a CoP to design the incentive schemes to enhance knowledge sharing practice in the community.

In our study, we considered the *competence* and *integrity* aspects of trust to understand the preference of the respondents towards knowledge sharing tasks in CoP [179]. The benevolence-based trust considers the self-motivation through a sense of moral obligation to become a part of a community. Therefore, the individual that receives the knowledge in the community does not play a significant role in influencing benevolence-trust of the person willing to share the knowledge. However, we are more interested in understanding the role of the trust established based on the action of the person receiving the knowledge, and not just from self-motivation.

We can also see the effect of social presence theory (SPT) [165] in the setting of

learning in communities of practice. The presence of other participants in CoP is essential because it enables direct or indirect contact with others. [70] explores the effect of SPT in the knowledge sharing behavior of the members of the virtual community and computer-mediated communication. In this study, we can see that the survey participant indicated that they prefer to communicate with the trusted party, whether face-to-face (offline) or by any other means. The perception of the high degree of social presence and having direct or indirect human contact contribute to the building of trust.

Knowledge is highly personal to an individual or a team [47]. There are several ways that people understand the meaning of privacy. In this study, we define privacy as "*control over the flow of one's personal information, including the transfer and exchange of that information*" [164]. People who perceive higher threats to privacy are less willing to disclose information about themselves as they have the fear to lose control of the information on the electronic platform [71]. In contrast, when the privacy policies are communicated and enforced, people perceive lower privacy risks, and they are willing to share more information [190]. The result of data analysis in this study affirms that the privacy concerns can act as the significant barrier to sharing knowledge, and the presence of privacy policy increase the willingness to share knowledge with the members of the community.

In our study, respondents were asked to state the influence of security on their knowledge sharing willingness in a CoP. The respondents in our study indicated that the lack of security, leakage of sensitive information act as the most severe barrier to their knowledge sharing willingness on CoP. However, our findings contradict the success of StackOverflow, a community of over 4 million programmers asking questions and providing answers in the field of Information Technology. In 2016, StackOverflow exposed the email addresses and phone numbers of the members of the community at inappropriate places due to a bug in their system [128] yet they succeed to pull experts from all across the globe to the community. Researchers argued that reputation [19] and emotion [135] play a major role in encouraging people to use StackOverflow.

10.7 Research limitations and future work

We used an online self-administered survey to collect response from the prospective members of UnRizkNow. Therefore, the questionnaire could be interpreted by the respondents according to their understanding in the given area, and it could influence their response. Furthermore, we collected the data from the participants who volunteered for it. It signifies that the response is collected from the people who had enough time and interest to complete the survey. The result might have differed if we had selected the participants randomly. However, the recruitment

process that we used in this study could not provide the provision to select the sample randomly. The study also inherits the limitation on the honesty of free-willed respondents. This is the main reason that we always considered the response stated by the respondents as 'stated preference.' The 'revealed preference' can be collected only through empirical study, i.e., by direct or indirect observation. Future research could endeavor to carry out this research approach.

10.8 Acknowledgment

This study is a part of UnRizkNow project, which is partially funded by CCIS. Adam Szekeres provided his useful input to formulate the questionnaire. Martin Stokkenes and Gaute Wangen helped us to translate the online questionnaire to the Norwegian Language. NorSIS supported our research work by distributing the survey to the people in the industry in Norway.

Chapter 11

Article 4: Factors influencing the participation of information security professionals in electronic communities of practice

Vivek Agrawal & Pankaj Wasnik & and Einar Arthur Snekkenes, Factors Influencing the Participation of Information Security Professionals in Electronic Communities of Practice. In Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Funchal, Portugal, pp. 50-60

11.1 Abstract

The purpose of this study is to contribute to a better understanding of the current status of the participation of the information security professionals (ISPs) in the electronic communities of practice (eCoP) in the information security (IS) domain in Norway. An online survey is conducted with 56 ISPs working in Norway to investigate this issue. This study used the logistic regression as a statistical technique to formulate the results and findings. The probability of an ISP being a user of eCoP is tested with demographic data, nature of the job, and the knowledge sharing preference. Furthermore, the determinants of the knowledge sharing theories, i.e., the theory of planned behavior, the motivation theory, and perceived trust the-

ory are used to test our statistical model. The findings of this study are useful to get the initial insight into the determinants that influence the participation of ISPs in eCoP in Norway.

11.2 Introduction

The ISPs working in different organizations in Norway often face many of the same problems and design similar solutions. ISPs also collect and apply the same knowledge to design their solutions. However, it is inefficient if they do it so largely on their own [57]. Therefore, proper sharing and reuse of knowledge among the ISPs can improve the quality of their work [185]. The involvement of information security practitioners and learning is an important cog in the wheel of knowledge translation. The knowledge available on the information security guidelines and journals is inadequate to solve the day-to-day problems faced by ISPs in their job. An evolving body of research suggests that communities of practice can be effective in engaging the professionals and enable the sharing of knowledge among them. The members discuss issues and learn from others' experience to solve the challenges in their job. The nature of the learning that evolves from these communities is collaborative, i.e., the collective knowledge of the community is greater than any individual knowledge [97], [115].

With the advancement in information and communication technologies, communities of practice adopted the possibility of virtual communication among the members of the community [80]. Modern information technologies can extend the boundaries and reach of these communities by providing an electronic platform to share knowledge in the community. The electronic communities of practice (eCoP) can establish collaboration across geographical locations and time zones. The adoption of eCoP is not restricted to any particular community or domain. The application of eCoP is spread across healthcare [80], finance sector [20], banking & Information Technology [148]. However, it is not explicitly evident whether eCoP is popular among the ISPs in Norway. We believe that sharing of knowledge among the ISPs improve IS in Norway. Therefore, we investigate the following research question in this study:

RQ1 What are the factors affecting the participation of information security professionals in electronic communities of practice in Norway?

This study contributes towards the understanding of the various factors that influence the participation of ISPs in eCoP in Norway. We are interested in investigating this issue because we want to establish an open electronic community of practice in IS for the ISPs. Therefore, it is imperative for us to learn the present status of participation of ISPs in eCoP as there is a lack of literature.

An online survey is conducted with the members of ISF, Norway. The participants of this survey are also the target audience (in the form of members) of the electronic community that we are interested in establishing. We collected the responses from the ISPs to understand the nature of their job, the source they use to collect essential information for their task, and the challenges they face in obtaining such information. Furthermore, we also collected their knowledge sharing preferences in eCoP based on the factors derived from the theory of planned behavior [16], motivation theory [62], and perceived trust [179]. The findings of this study act as a starting point to get an initial insight into the popularity of eCoP among ISPs in Norway.

The rest of the paper is structured as follows: In section 11.3, the existing literature is used to describe the concepts and knowledge sharing in eCoP. In section 11.4, the research approach of the study is explained. In section 11.5, the findings of the study is explained with the help of survey responses. Finally, the paper ends with a discussion of the results, stating the implication of the findings, limitation of the study and expected future work, and the conclusion.

11.3 Related work and background knowledge

This section presents an overview of the difference between traditional CoP and eCoP followed by the studies covering the knowledge sharing activities in eCoP.

11.3.1 Traditional vs electronic Communities of Practice

The term 'communities of practice' (CoP) is introduced by Wenger et al. in 1998 [191]. The basic concept of CoP is presented by Lave & Wanger [109], and by Brown & Duguid [31] in 1991. According to Wenger [192], "*Groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis*" A CoP mainly consists of three fundamental elements: a) *Domain* creates common ground and sense of common identity. A well-defined domain enables the community to understand its purpose and value to the members and stakeholders associated with the community, b) *Community* creates the bond among the members that enable the learning among them. A strong community can be developed when the members have mutual respect and trust among them. A strong community also encourages healthy interactions and discussion, c) *Practice* is the specific knowledge the community develops, shares, and maintains. A practice can be a set of ideas, tools, information that the community members share [192].

A CoP can exist in offline (also known as traditional) or electronic or both the forms. The offline form uses face to face meeting, roundtable discussion, whereas the electronic form uses networked technology, mainly the Internet, to establish

collaboration among the members across the world. The idea of having an electronic platform for the traditional communities of practice is supported in the studies [121], [194]. The traditional communities rely heavily on the location and have membership according to norms. The electronic communities are organized around an activity, idea or task rather than location [97]. The electronic nature of the community provides the opportunities to facilitate communication among the members from different geographic locations and time zones. The electronic CoPs combine both online activities and face to face meetings to enhance the interaction process.

11.3.2 Knowledge in electronic communities

According to the work of [189], there are three perspectives of knowledge on the definitions of knowledge, i.e., *Knowledge as object*, *knowledge embedded in individuals*, and *knowledge embedded in a community*. In this study, we focused on the third perspective, i.e., knowledge embedded in a community to define the knowledge sharing practice in eCoP. The community perspective of knowledge can be used to develop and support electronic communities of practice. This perspective defines knowledge as 'the social practice of knowing' [161] and argues that learning, knowing and innovating are closed related forms of human activity and inevitably connected to practice. The knowledge resides in a community can be used to enable discussion, and share ideas among the members of eCoP.

Moreover, the use of information and communication technologies enables knowledge sharing through the mechanisms that allow sharing incidence based on personal experience, discussing and debating issues related to the domain of the community, posting and responding to the queries [189]. In eCoP, the knowledge can be stored in the digital form and transferred to others regardless of the location of the individual who generated the knowledge and who is going to receive it. Knowledge sharing in eCoP is a process that exploits existing knowledge by identifying, transferring, and applying to solve tasks better, faster and cheaper [41]. However, members are often reluctant to share knowledge of others in the eCoP [175].

Furthermore, Ardichvili et al. [20] conducted a qualitative study to understand the motivation and barriers to participating in eCoP at Caterpillar Inc. The study identified that the members of the community are not willing to share their knowledge because of the fear of criticism or misleading the other members. It has been shown in a recent study [12] that the participants (IT professionals) of the communities were not willing to participate actively in the absence of strong motivation. ISPs may not want to disclose information on eCoP that describes their organization's security status or any weakness. Therefore, it is important to anonymize the knowledge sharing process [57]. The role of trust in encouraging the

ISPs to share knowledge in eCoP is studied in [64], [154], [57].

11.3.3 Underlying theories

This study considers knowledge sharing behavior and participation of ISP in eCoPs as an individual's social psychological process. Thus, one's attitude, intention, motivation, trust subsequently influence the behavior of the individual. We adopted three theories in this work to analyze the factors affecting the participation of ISPs in eCoP. The theories are as follows:

11.3.3.1 Motivation Theory (MT)

Motivation refers to "internal factors that impel action and to external factors that can act as inducements to action" [118]. According to Fray et al. [139], motivation to share knowledge is driven by intrinsic and extrinsic factors. Extrinsic motivations satisfy the instrumental needs of a human. For instance, money, financial reward, social rewards, increase in the status. Intrinsic motivations are perceived by the values provided directly within the work [62]. For instance, altruism drives many people to do something for the enjoyment of doing the work.

11.3.3.2 Theory of Planned Behavior (TPB)

According to TPB theory, the human behavioral intentions are determined by three factors: attitude, subjective norms, and perceived behavioral control. Attitude refers to the degree to which one evaluates the behavior favorably or unfavorably. Subjective norm is the perceived social pressure to perform or not perform the behavior. Perceived behavioral control is defined as the degree to which a person perceives that the decision to engage in a given behavior is under his/her control [95].

11.3.3.3 Perceived Trust theory (PTT)

The role of trust in increasing the willingness to share knowledge in an online community of practice is studied in [179] where trust is conceptualized into *competence*, *integrity*, and *benevolence*. Competence-based trust defines the degree to which a member believes that the community is knowledgeable and competent. Integrity-based trust defines the degree to which a member believes the community to be honest and reliable [122]. The *benevolence* trust considers the self-motivation through a sense of moral obligation to become a part of a community. Therefore, the individual that receives the knowledge in the community does not play a major role in influencing benevolence-trust of the person willing to share the knowledge. However, we are more interested in understanding the role of the trust that is established based on the action of the person receiving the knowledge, and not just by self-motivation.

11.4 Research Method

This study is based on the principle of *stated* preference technique [32] for establishing valuations. An online survey-based technique is designed to collect the response from the ISPs. The online questionnaire is distributed in one of the ISF meetings where 56 ISPs participated in answering the survey.

11.4.1 Questionnaire design

An online quantitative questionnaire was created using LimeSurvey open source survey tool. The questionnaire was posted on the project website [7]. The online survey was available in both English and Norwegian. The respondents accessed the online survey on their smartphone during the ISF meeting. The survey consisted of 18 questions covering the topics on demography, working activities, and preference for eCoP. The detail of the survey is given in 15.3. The survey was conducted at the Information Security Forum (ISF) Norway meeting. The questionnaire consists of three sections that are as follows:

1. *Demography* - Questions related to age, gender, job role, job location, type of organization, the size of an organization.

2. *Work activities* - Questions related to daily tasks, full-time or half-time ISP, the source used to collect information, challenges associated with information gathering.

3. *Community-based knowledge sharing* - Questions on prior experience using eCoP, the nature of eCoP, no. of members on eCoP, the domain of eCoP, and the preferences related to sharing knowledge, participation on eCoP. This part of the questionnaire is created to analyze the concepts of the theories mentioned above (Ref. section 11.3.3).

11.4.2 Respondents

A total of 56 respondents (46 male, 9 female, 1 undisclosed) volunteered to complete the online survey. The majority of the respondents were working as a full-time ISPs in Norway. A short introduction to the research project was presented to the respondents at the beginning of the workshop. The objective of the online survey and the details of the various terms, used in the questionnaire, were also presented to the survey respondents. The survey had the option for the respondents to decline their participation at any point in time if they feel uncomfortable participating in the survey.

Table 11.1: Summary of the demographic data of ISPs participated in the survey

	age	sex	edu_level	ocp_level	no_emp	no_hrs
1	$>60:5$	Female: 8	Asso. degree : 7	Unspecified : 1	5000- :13	0-10 : 6
2	21-30: 3	Male :40	B. degree :13	Administrative: 2	1000-4999:11	11-20: 6
3	31-40:14		Doc. degree : 3	CISO :13	100-499 : 7	21-30: 6
4	41-50: 9		HS diploma : 2	Other :19	0-10 : 6	31-40:17
5	51-60:17		M. degree :19	Researcher : 2	10-49 : 3	41- :13
6			Other : 2	Security Engineer :11	50-99 : 3	
7			Tech. training : 2		Other : 5	

11.4.3 Data analysis

We collected data from 56 respondents through the online survey. Since the study was restricted to the users participating in only in the online CoPs, we rejected the responses of six respondents as these respondents participated only in the offline communities of practice. Subsequently, we rejected two more observations from the sample as they did not answer many questions in the questionnaire. Therefore, our final sample size consisted of 48 observations. A dichotomous data was considered as an output variable with the values, 'yes' and 'no,' which signifies whether the given user participates or does not participate in eCoP respectively. Based on the study and argument presented in the studies [116], logistic regression fit well with this study. Ergo, logistic regression (also called logit) was used as a statistical technique to formulate the results and findings. Hence, all predictors were considered as categorical variables whereas the participation in eCoP (Y_i) was assumed as a dichotomous or binary outcome. Furthermore, this study assumed the covariates such as age, gender, educational levels, occupational levels, the organizational size of the respondents and the number of hours spent on IS per week as independent variables. Equation 12.1 summarizes the main element of the logit model and Equation 11.2 expresses the probability of Y_i.

$$Y_i = \begin{cases} 1 & if\ the\ i^{th}\ subject\ is\ using\ eCoP \\ 0 & otherwise \end{cases} \tag{11.1}$$

$$y_i = p(x_i') = \frac{exp(\beta_0 + \beta_1 x_{1i} + \beta_2 x_{2i} + ... + \beta_n x_{ni})}{1 + exp(\beta_0 + \beta_1 x_{1i} + \beta_2 x_{2i} + ... + \beta_n x_{ni})} \tag{11.2}$$

where

- y_i can be considered as realization of output variable Y_i which takes the values 1 or 0 with probability value of p and $1 - p$ respectively.
- x_i' is i^{th} vector of the independent variables as mentioned earlier.

- $\beta_0, \beta_1, \beta_2, \ldots, \beta_n$ are the coefficients of fitted regression models.

Equation 11.2 can be rewritten as log-linear function as given below which is further used in deducing the final output.

$$\begin{aligned} logit(Y_i) &= log\frac{p(x_i')}{1-p(x_i')} \\ &= \beta_0 + \beta_1 x_{1i} + \beta_2 x_{2i} + ... + \beta_n x_{ni} + \epsilon \end{aligned} \tag{11.3}$$

Furthermore, we formulated the decision rule as, the negative values of the logit of output variable will result into non user of the eCoP whereas positive logit value will represents the user of eCoP.

11.5 Research Results

This section provides the statistical results of the logistic regression model fit which is formulated to investigate the research question RQ1 in this study.

11.5.1 Result I

The information about the demography of the ISPs members is presented here. Table 11.1 tabulates the statistics of the collected data. There are 35 ISPs with university-level education, i.e., an education degree in bachelors, masters or doctorate in Information security and allied branches. The majority of the respondents are males in the age group of 30 - 60 years. 75% of the respondents work full-time in IS domain mainly affiliated to Information and communication industry, Financial and insurance, business service, health and social services sectors. Our findings also highlight that the ISPs in our survey come from small (employee strength 1-19), medium-sized (20-99) and large (100+) companies [93].

11.5.2 Result II

Based on the Equations 11.2 and 11.3, we have modeled our data by fitting logistic regression model using R software [149]. In this model, we considered four independent variables which are *age*, *gender*, *no. of employees* and *no. of hours* spent on IS related tasks[1]. Table 11.2 presents the coefficients and the significance of these variables. We can see that the categorical variable *no. of employees* have all positive coefficients, which indicates that the unit increment in the *no. of employees* encourage the participation in eCoP whereas the *no. of hours* spent on task related to IS has the negative coefficients. Ergo, it can be inferred that the participation of ISPs, who work full-time or more in IS task, is low in eCoP.

[1] All explanatory variables considered here are categorical variables

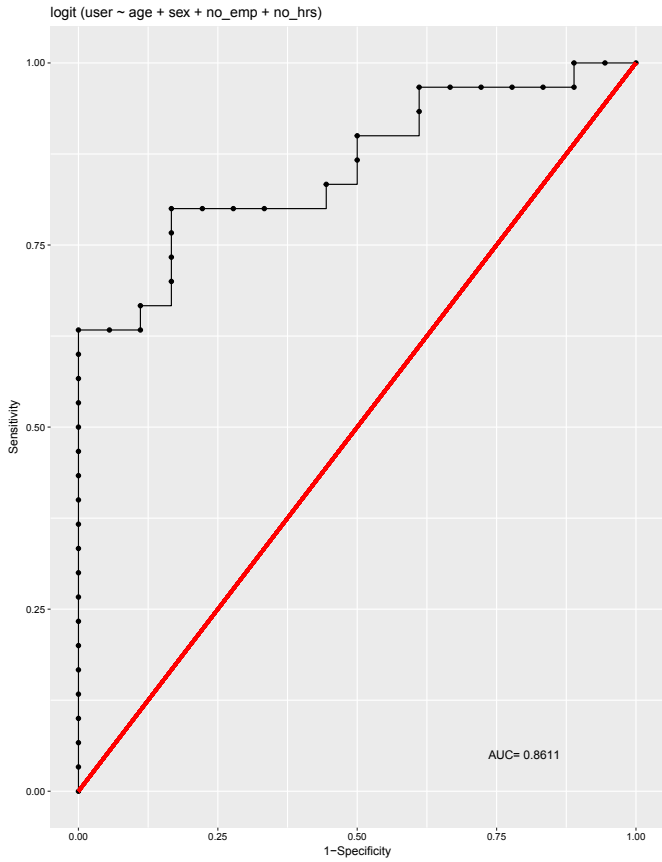


Figure 11.1: ROC curve for logistic regression model

To test the significance of these explanatory variables, under the null hypothesis all the coefficients will take the value equal to 0. For example, $H_0 : \beta_1 = \beta_2 \cdots = 0,\ and\ H_a :\neq 0$

From the Table 11.2, p-value for levels no_emp100-499(β_p) and no_emp1000-4999(β_q) is 0.05 which is statistically significant [2]. Hence, H_0 is rejected in the study. The p-value of no_hrs31-40(β_r), no_hrs41(β_s) is 0.03 and 0.09 which shows that levels have significant effect on the probability of participating in eCoP. Hence, the output variable can be explained in terms of the odds ratios which can be obtained by calculating the exponential of $\beta_p, \beta_q, \beta_r, \beta_r$ i.e $e^{\beta_p} = 100,\ e^{\beta_q} = 63,\ e^{\beta_r} = 0.0075,\ and\ e^{\beta_s} = 0.0252$. Therefore, we can write that:[3]

- On average, for every one unit change in the number of employees, the log odds of being a user of eCoPs (versus non-user) increases by 81.2.
- For a unit increase in the number of hours spent on tasks related to the IS per week, the log odds of being the use of eCoPs increase by 0.0164.

The variables age, gender have a slightly different interpretation. For all age groups, the obtained p-value is significantly high with an average value of 0.69 hence we can not reject the H_0. In addition to this, we can see that the most of the variables are statistically non-significant. Thus, we can consider that the probability of participating in eCoP is not affected by the demography factors such as age, gender, and educational level. Further, we used Receiver Operating Curve (ROC) and area under the ROC curve (AUC) to report the performance of the fitted model. ROC Curves describes how well the fitted model can separate the two classes 0 and 1, and it also helps to identify the best threshold for separating them. In the case of ROC curves, the AUC plays an important role; higher the AUC better the model in classification. Figure 11.1 represents the ROC of the fitted logistic regression model and AUC = 0.86, which can be considered as high performance for real-life applications.

11.5.3 Result III

In this section, there are three factors related to work activities of ISPs analyzed to see their effect on the probability of ISPs in participating in eCoP. The factors are *source of obtaining information required to do the professional tasks*, *nature of the tasks*, and *the challenges faced in obtaining the information*. The details of the factors and their variables can be obtained from Appendix 15.3.

[2] We considered significance at 90% confidence level

[3] Analysis is made on the basis of explanatory variables which are statistically significant, non significant variables can be excluded and one can remodel the system

Table 11.2: Summary of estimated logistic regression model

Var.	Coef	S.E.	z-val	Pr(>|z|)
(Int.)	0.85	3.51	0.24	0.81
age21-30	19.03	2935	0.01	0.99
age31-40	-2.90	2.62	-1.11	0.27
age41-50	0.32	2.72	0.12	0.91
age51-60	-1.35	2.52	-0.54	0.59
sexMale	2.04	1.35	1.51	0.13
no_emp10-49	0.12	2.63	0.05	0.96
no_emp100-499	4.63	2.33	1.98	0.05*
no_emp1K-4.9K	4.14	2.12	1.95	0.05*
no_emp50-99	0.91	2.01	0.45	0.65
no_emp5K-	3.11	2.06	1.51	0.13
no_empIDK	0.85	2.09	0.40	0.69
no_hrs11-20	-3.22	2.44	-1.32	0.19
no_hrs21-30	-1.69	1.95	-0.87	0.38
no_hrs31-40	-4.90	2.26	-2.17	0.03*
no_hrs41-	-3.68	2.16	-1.70	0.09*

Table 11.3[4] shows that the variables [S1-S8] of 'source of information' have positive coefficient which signifies that the unit increment in the motivation will increase the participation of ISPs in eCoP. Variable S3 has a statistically significant effect on the participation of ISPs in eCoP. Variable S3 signifies that respondents, who ask other professional experts on communities of practice to obtain necessary information to carry out their task, also participate in eCoP. In a case of the usual activity that ISPs perform their job tasks, the variable N7 has statistically significant (p-value less than 0.1) effect on the participation of ISPs in eCoP. The challenges, which are faced by ISPs in obtaining the information for their job, do not have a statistically significant effect on eCoP participation. It also signifies that we cannot predict the probability of ISPs participating in eCoP by having any information on the challenges that they face within the category given under C1-C6.

11.6 Discussion

Knowledge sharing is an intentional behavior which cannot be forced by someone [63]. People participate in eCoP to exchange knowledge with the others. Therefore, it is useful to analyze the knowledge sharing behavior of ISPs in eCoP. The

[4]The variable corresponding to Reference modality is automatically considered as a reference by R GLM package

Table 11.3: Summary of variables under information source, nature of job tasks, and challenges in obtaining information

Var.	**Coef**	**S.E.**	**z-val**	**Pr(>|z|)**
(Int.)	11.37	3840.09	0.00	1.00
Source of information				
S1	0.91	1.51	0.60	0.55
S2	Reference modality			
S3	4.77	2.15	2.22	0.03*
S4	Zero entry in the response database			
S5	1.11	1.69	0.66	0.51
S6	0.62	1.86	0.33	0.74
S7	2.99	9224	0.00	1.00
S8	0.12	2.01	0.06	0.95
Nature of tasks				
N1	21.73	6522.64	0.00	1.00
N2	3.38	2.17	1.55	0.12
N3	Reference modality			
N4	3.13	2.22	1.41	0.16
N5	2.49	2.41	1.03	0.30
N6	2.06	2.44	0.84	0.40
N7	5.05	2.66	1.90	0.06*
N8	20.94	6522.64	0.00	1.00
Challenges in obtaining information				
C1	-14.66	3840.08	-0.00	1.00
C2	-17.53	3840.08	-0.00	1.00
C3	3.07	5989.08	0.00	1.00
C4	-18.16	3840.08	-0.00	1.00
C5	-19.26	3840.08	-0.01	1.00
C6	Reference modality			

factors, affecting the participation of ISPs in eCoP activities, are investigated with the help of **MT**, **TPB**, **PTT** (refer section 11.3.3). We modeled our data by fitting the logistic regression model. In this model, we considered the variables of **TPB**, **MT**, and **PTT** to predict the probability of participating in eCoP. The variables are defined in the online questionnaire given in the Appendix 15.3.

11.6.1 Motivation Theory

Table 11.4 presents that the determinants of *motivation* have positive coefficients, which indicate that a unit increment in the motivation will increase the participation of ISPs in eCoP. We considered seven factors under the motivation theory. SQ05 corresponds to intrinsic motivation, and SQ08, SQ10, SQ11, SQ13, SQ15, SQ20 are extrinsic motivation. Out of 7 variables, only the p-value of SQ08 is less than 0.1.

Table 11.4: Summary of the variables under Motivation Theory

Var.	**Coef**	**S.E.**	**z-val**	**Pr(>|z|)**
Motivation				
(Int.)	-1.44	0.84	-1.72	0.09
SQ05	0.17	0.77	0.22	0.83
SQ08	1.31	0.72	1.82	0.07*
SQ10	0.60	0.88	0.69	0.49
SQ11	0.41	0.74	0.55	0.58
SQ13	0.68	0.76	0.90	0.37
SQ15	0.73	0.71	1.02	0.31
SQ20	0.62	0.90	0.69	0.49

Therefore, it can be concluded that SQ08 has a statistically significant effect on the participation of ISPs in eCoP. The ISPs tend to participate in eCOP more if members in the community share information relevant to them. It can be considered as one of the main incentives for the ISPs as well.

11.6.2 Theory of planned behavior

Table 11.5 presents the summary of the three major determinants of TPB, i.e. *attitude*, *subjective norm*, and *perceived behavioral control*. We can see that the variable SQ01, SQ06, SQ12, SQ14, and SQ22 have positive coefficients, i.e., the unit increment in these variables will signify the increment in the participation of ISPs in eCoP. The p-value of the variables SQ22 and SQ12 is less than 0.1. Hence, SQ22 and SQ12 have a statistically significant effect on the participation of ISPs in Norway in eCoP. SQ22 corresponds to the statement *'my organization allows me to participate in a community-based platform to share my knowledge'* in the questionnaire.

Table 11.5: Summary of variables under the Theory of Planned Behavior (TPB)

Var.	Coef	S.E.	z-val	Pr(>|z|)
Subjective norm				
(Int.)	0.13	0.48	0.26	0.79
SQ14	-0.09	0.78	-0.12	0.91
SQ22	2.16	0.88	2.44	0.01*
Attitude				
(Int.)	0.51	0.52	0.99	0.32
SQ01	16.26	1455.40	0.01	0.99
SQ06	0.08	0.65	0.12	0.91
SQ07	-1.20	1.33	-0.91	0.37
Perceived behavioral control				
(Intercept)	-0.37	0.43	-0.85	0.40
SQ12	1.80	0.66	2.73	0.01*

In other words, the participation of ISPs in eCoP can be decided by investigating if the organization has any restriction on the employee to participate in eCoP. SQ07 corresponds to the negative feelings about knowledge sharing in eCoP [*I do not share anything as I am concerned about the sensitivity of my information*]. SQ07 is the only variable with the negative coefficient, which signifies that the unit increment in this variable will reduce the participation of ISPs in eCoP. It can be learned from applying TPB concepts that the variables of the subjective norm and perceived control behavior are the important factors in influencing the participation of ISPs in eCoP.

11.6.3 Perceived trust

In our study, we considered the *competence* and *integrity* aspects of trust to understand the preference of the respondents towards knowledge sharing tasks in eCoP.

Table 11.6: Summary of the variables under Perceived Trust concept

Var.	Coef	S.E.	z-val	Pr(>|z|)
Perceived Trust				
(Int.)	0.044	0.49	0.09	0.93
SQ18	1.11	0.68	1.65	0.10*
SQ19	-0.08	0.62	-0.14	0.89

Table 11.6 presents the findings of the variable related to Trust factor. SQ18 and SQ19 have the positive coefficient and hence has the positive effect on the participation of ISPs in eCoP. Moreover, SQ18 is also statistically significant in predicting

the ISPs' participation.

11.7 Conclusion

The main objective of the present study was to understand the present status of the participation of ISPs in Norway in eCoPs in IS. To achieve this goal, we analyzed various factors that help us predict the participation of ISPs in eCoP.

In this study, we observed that the number of employees in the organization, and working hours in the security area are the significant factors in predicting the participation in eCoPs. Further, we observed that both extrinsic and intrinsic motivation is positively correlated with the participation in eCoP. The finding of logistic regression points out that the participation of ISPs in eCoP is statistically influenced by the factor that other members of the community share relevant information on the problems of ISPs. In other words, we can expect high participation if we can ensure that the members of the community will share information that is useful to the participants. However, the tendency to share knowledge decreases when it is perceived that they are receiving irrelevant or not so useful information from other members.

The application of TPB also led to some important observation in this study. The probability of the participation in eCoP is significantly increased if the organization encourages the employee to participate in the knowledge sharing activities. Typically, eCoP needs information technology capabilities to establish the knowledge sharing process. The presence of the necessary resources (in the form of platform, and service) also enables the ISPs to participate in eCoP.

11.8 Research limitation and future work

The response that we received from 48 participants provides an initial insight into understanding the current status of participation in electronic communities of practice by ISPs in Norway. However, the findings cannot be generalized to a large population because of the small sample size of the respondents. Hence, more studies are needed to generalize present study findings. Furthermore, we collected the data from the participants who volunteered for it. It signifies that the response is collected from the people who had enough time and interest to complete the survey. The result might have differed if we had selected the participants randomly. The future research will address this issue by targeting large respondents and selecting a random sample from it.

In our study, we mainly tried to understand the preference of the members who are going to share their knowledge. The receiver's perspective is also essential in the context of knowledge sharing task. Future research will aim to address this

issue by collecting the perspective of both the parties. It will help to compare their preference and design the incentive scheme along with the sharing model. The use of categorical variables in the logistic regression model can also cause some issues. Therefore, we are investigating the possibility of adopting a linear scale in the future data collection events.

Chapter 12

Article 5: UnRizkNow - An open electronic community of practice for information security professionals

Vivek Agrawal & Einar Arthur Snekkenes, UnRizkNow: An open electronic community of practice for information security professionals. In Proceedings of the 2017 9th International Conference on Education Technology and Computers (ICETC 2017). ACM, New York, NY, USA, 191-197

12.1 Abstract

We are establishing UnRizkNow as the open electronic community of practice (eCoP) for information security practitioners (ISP) working in Norway. UnRizkNow will be helpful to solve the challenges faced by the ISP in the information security domain. The purpose of this study is to analyze the factors that are essential to design the information sharing features of UnRizkNow. A research model based on purpose, motivation, facilitating condition, and preference to share knowledge in the electronic platforms is proposed in the study. Furthermore, an online questionnaire is developed based on the elements of the proposed research model to collect responses from the ISP affiliated with ISACA Norway. We analyzed the responses collected through the online survey to extract the most desirable features of UnRizkNow community. We incorporated several features into UnRizkNow such that: a) the information available in the community is easy to search, b)

the updated information can be easily accessed, c) verify the information is coming from a reliable member, d) The information is relevant to the problem/concern of the member, e) all the useful information can be collected at the same place. The designed features of UnRizkNow will be helpful for ISP to share knowledge effectively.

12.2 Introduction

Information security professionals (ISP) often face many of the same problems in their day-to-day job. They also collect and apply the same knowledge to design their solutions. However, it is inefficient if they do it so largely on their own. The knowledge available in the guidelines, and the documents released by the security standards are inadequate to solve the day-to-day problems faced by ISP. We believe that proper sharing and reuse of information security (IS) knowledge among the ISP can improve the quality of their work and help them design security solution effectively [185].

There are several ad-hoc groups available on LinkedIn, and Facebook dedicated to information security related topics. However, the existing groups lack the active members who share relevant knowledge regularly. The knowledge available in these groups are not updated regularly, or the topic of the knowledge is irrelevant to most of the members. Thus, an open electronic community of practice can be useful in collaborating with the IS professionals and enable the sharing of essential IS knowledge among them. Therefore, we aim to establish an open electronic community of practice (eCoP), UnRizkNow, for ISP working in Norway. We are putting in our effort to understand the underlying factors that can help us to address the shortcoming of the existing communities and design the features of UnRizkNow. Therefore, we investigate the following research question in this study:

RQ1 How can an electronic community of practice for information security professionals be established in Norway?

In this study, IS knowledge refers to all intelligible ideas, information and data in whatever form in which it is expressed or obtained in the field of Information Security. IS knowledge required by information security professionals to carry out their regular tasks. IS knowledge can be - a) A method to compare different risk management methods, b) Details of risk assessment phase, c) Details of new anti-virus installed in the organization, d) The reports on IS incidents

This study contributes to our understanding of the various factors that are imperative in establishing UnRizkNow in information security. A research model is constructed to investigate various factors related to the motivation, purpose, facil-

itating conditions, and preference to share IS knowledge in the electronic platform. Afterward, an online survey is designed to collect responses related to the factors mentioned in the research model. The online survey is conducted with a small group of ISP affiliated as the ISACA members in Norway [90]. The findings of the online survey guided us to design the information sharing features, incentive schemes, and reputation scheme of UnRizkNow platform.

The rest of the paper is structured as follows: Section 12.3, presents an overview of UnRizkNow community using the fundamental concepts of community of practice. Section 12.4 presents the research model of this study, the details of questionnaire design and data analysis approach. Section 12.5 presents the details of the analysis performed on the survey response data. Section 12.6 describes the useful features of UnRizkNow community that are adopted in this study. Finally, the paper ends with the limitation of the study and expected future work, and the conclusion.

12.3 Overview of UnRizkNow

UnRizkNow is to be established as an open electronic community of practice for the information security practitioners in Norway. Unlike closed community of practice, an open community does not restrict the membership based on member's affiliation or other such factors [11]. The behaviors of information security students towards knowledge sharing activities on UnRizkNow is studied in [12]. Descriptive theories like - Social exchange theory (SET) [52], Theory of motivation and barriers (TMB) [21], social presence theory (SPT) [166], Theory of planned behavior (TPB) [16] are analyzed to explain the knowledge sharing behaviors of the students. Agrawal et al. [6] identified the underlying risks that can affect the normal operation of the community. It adopted the CIRA [151] approach to analyzing the risks that can be generated in the community because of the conflicting incentives between the members and the organizer of the community.

UnRizkNow can be defined in variety of forms that any traditional community of practice may take. However, we stick to the basic representation of CoP based on the [192] structural model. UnRizkNow consists of three fundamental elements: a) *Domain*, b) *Community*, c) *Practice*. Figure 12.1 shows the details of the structural model of UnRizkNow community.

The objective of UnRizkNow is to identify relevant challenges that ISP face in their field of interest and enable them to resolve these challenges by sharing knowledge in the form of ideas, answers, and experience in the community. The topics of the community are related to challenges in the Information security field. The members of the community are encouraged to share their knowledge in the area

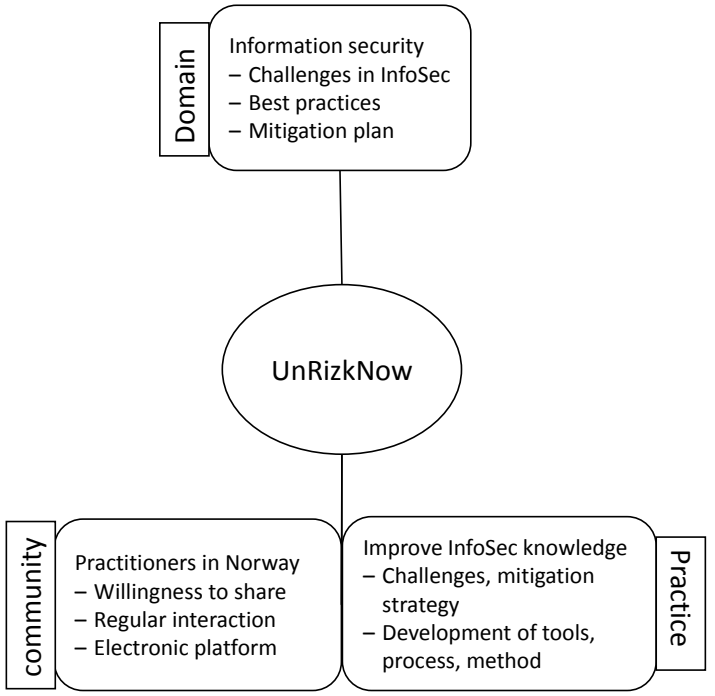


Figure 12.1: The structural model of UnRizkNow community

of InfoSec to solve the challenges/problems of the other members. The scope of the domain is not a constant entity, and it evolves as the community evolves. Thus, the primary objective of UnRizkNow is to define the domain in a way it can identify and engage the potential members initially. The aim of defining the scope of the domain should not be directed towards determining the final shape of the community in the very initial stage.

The UnRizkNow community consists of ISP working in Norway in small-sized to large enterprises. The members must actively work part-time or full-time in the area of information security. UnRizkNow can consist of participants having different roles in the community, e.g., Sponsor, organizer, member, Facilitator, leader [6]. However, we want to focus only on the members' role in UnRizkNow community in the beginning. The community is mainly dependent on the willingness to share knowledge among the members [11], incentive [110], trust [55], and mutual respect among the members. The electronic community will allow the members to connect through the online platform available on the web domain. Therefore, the members can regularly interact without having the necessity of meeting face to face. The members can post their concerns/problems under the relevant section of the community. Members can their true-identity or use nickname while sharing their knowledge on UnRizkNow.

The members of UnRizkNow community will practice regularly to improve their knowledge in the information security domain. The practice will be focused to share the challenges/problems, and mitigation strategy that ISP face in their work. A practice can be a set of ideas, tools, cases and stories, theories, rules, models, and best practices that the community members share [192]. UnRizkNow should allow the members to share documents, web articles in the form of knowledge repositories that members share.

12.4 Research method

A research model is designed to conduct this study. The research model is based on the idea of knowledge sharing behaviors presented in the studies [12], [11]. An online questionnaire is designed to collect the information of the elements involved in the research model. The online questionnaire is distributed at ISACA meeting event in Norway. A total of 28 members participated in answering the questionnaire. The features necessary to establish UnRizkNow community are described based on the responses collected through the online questionnaire.

12.4.1 Research model

Figure 12.2 presents the research model for this study. This model consists of four essential parts that are necessary to establish an eCoP in information security. The

elements in the research model help to design the sharing rules, incentive schemes, and technical features of UnRizkNow community.

The *first* part of the model identifies the purpose of sharing IS knowledge on the electronic community of practice. We believe that members mainly share their knowledge either to learn about a specific skill, solve a given problem; educate/inform others by providing necessary information.

The *second* part of the model identifies the factors that motivate the members to share the IS knowledge on eCoP. We applied the theory of motivation to understand its role in the establishment of a successful electronic community of practice for the ISP in Norway. Motivation refers to "internal factors that impel action and to external factors that can act as inducements to action" [118]. According to Fray et al. [139], motivation to share knowledge is driven by intrinsic and extrinsic factors. Extrinsic motivation meets the instrumental need of a human, i.e., money, financial reward, increase in the status. Intrinsic motivation is perceived by the values provided directly within the work [62]. Intrinsic motivation has been associated with the creativity of performance, longer-lasting learning, and perseverance.

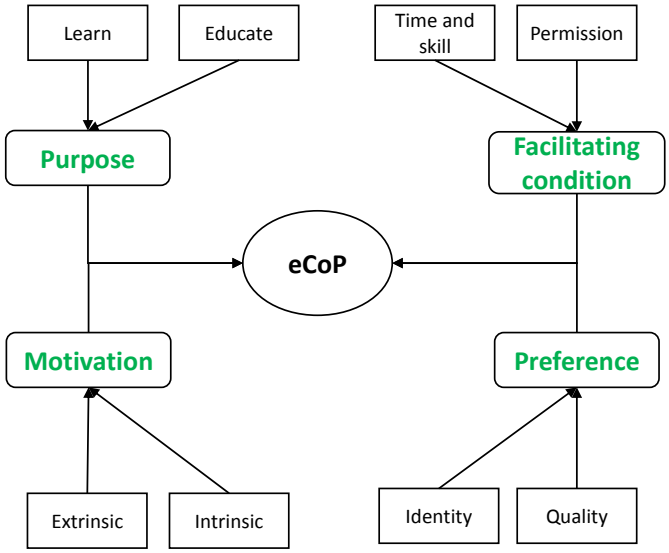


Figure 12.2: An overview of the research model based on purpose, motivation, facilitating condition, and preference

The *third* part of the model defines the facilitating conditions are the support systems enabled by the organization or by self. The support in the form of providing enough information systems, encouraging certain behaviors [95]. We categorized

the facilitating condition into permission and time & skill. It is often required to have special permission from the organization to share a part of the information with other due to the security requirement of the organization. Additionally, members need enough time and skill to participate actively in knowledge sharing tasks in eCoP. The nature of the job also plays an active role in facilitating the knowledge sharing activity.

The *final* part of the model define the preference regarding the sharing, reusing the knowledge on eCoP. We believe that the identity of the members can influence the knowledge sharing behaviors of the members. According to the theory of social exchange [52], individuals evaluate the perceived ratio of benefits to costs and plan their actions to maximize their benefits. In the setting of eCoP knowledge sharing, members can participate in knowledge sharing activity if they receive good-quality information from the other member of the community. Therefore, it is important for UnRizkNow community to have a mechanism/scheme to find good-quality information.

12.4.2 Questionnaire Design

A free open source software survey tool, LimeSurvey, was chosen to create an online quantitative questionnaire survey. The survey was hosted on our project website. The respondents accessed the online survey on their smartphone/tablet PC during the ISACA meeting. The survey consisted of 15 questions that assessed the demography, incentive, purpose, preferences for using eCoP to share IS knowledge. The survey had the option for the respondents to decline their participation at any point in time if the respondents feel that the answers might breach their privacy. The detail of the survey is given in the section 15.4.

12.4.3 Data analysis

The final sample size consists of 28 observations collected through the online questionnaire. We used IBM SPSS Statistics 24 (licensed) to analyze the survey response. Five-point Likert scale (1= is Strongly Disagree, 5=Strongly Agree) is used throughout the questionnaire. The idea of using a Likert-type scale in this survey is derived from the work of [175]. The mathematical model in our survey design assumes that the interval between values is not interpretable (i.e., the distance between 1-2 is not the same as the distance between 4-5). Therefore, calculating the mean or standard deviation of the given data is not a suitable approach to building any conclusion. Hence, the conclusion is derived based on the percentage of the respondents agree or disagree with the given statement. Equation 12.1 summarizes the logic used in this study to justify if the respondents agree or disagree with a statement in the online questionnaire.

$$Res_i = \begin{cases} Agree & if\ P(S_4) + P(S_5) >= 50\% \\ Disagree & if\ P(S_1) + P(S_2) >= 50\% \end{cases} \tag{12.1}$$

where

- S_1 = Strongly Disagree, S_2 = Disagree, S_3 = Undecided, S_4 = Agree, S_5 = Strongly Agree are the points on the Likert scale
- $P(S_n)$ denotes the percentage of the participants selected S_n point on the Likert scale.
- Res_i is the response of a participant for a given statement i in the online questionnaire. It can take value either agree or disagree.

12.5 Research Results

In this section, the answers collected during the online survey is analyzed to get an insight into the demography, purpose, and motivation to share the knowledge in eCoP. Further, we also analyzed the responses to understand the preferences and the role of facilitating conditions to influence the participation in eCoP.

12.5.1 Result I - Demography

This section provides the information about the demography of the ISP members participated in the survey at the ISACA meeting. A total of 28respondents (20 males, 7 females, 1 undisclosed) participated in completing the online questionnaire at the ISACA meeting. The majority of the respondents were between the ages of 41-50 years (43%). Figure 12.3 presents the profession/job role of the respondents. Most of the members work as the security consultant and auditor in Norway. A few of the members are risk advisor, CISO, sales manager, and Legal Adviser.

Most of the respondents (53%) work at least as a full-time information security professional in Norway ranging from small-sized companies to large enterprises. 35% of the members work as a part-time in the information security area.

12.5.2 Result II - Purpose and Motivation

This section provides the details of the purpose of sharing IS knowledge on eCoP and the factors that motivate the member to share their knowledge with the other members. We divided the purpose of sharing IS knowledge of eCoP into two broad categories, i.e., Learn and educate. We believe that members participate in

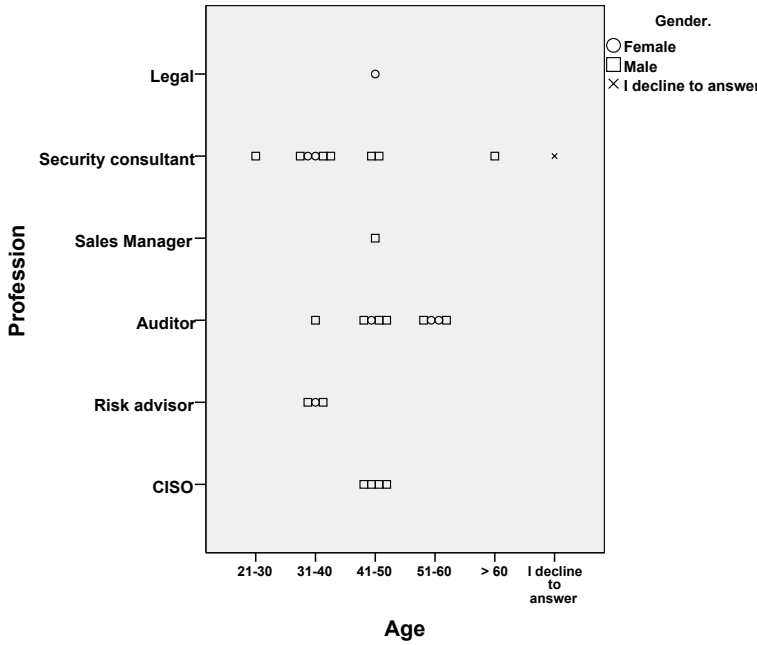


Figure 12.3: The profession, age and gender of the members who participated in the survey

knowledge sharing activities on the electronic platform either to learn or to educate others or to do both.

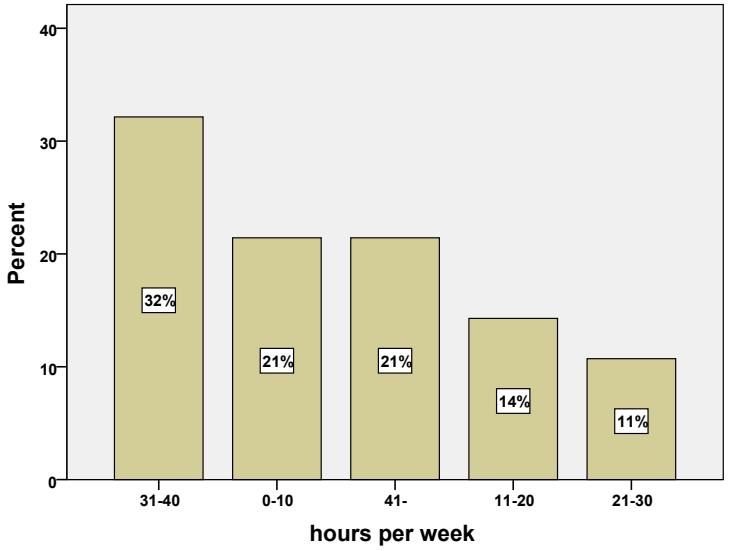


Figure 12.4: The amount of hours spent per week on the information security task by the respondents

Figure 12.5 shows that 89% of the respondents agree with the fact that they share IS knowledge with their colleagues on the electronic platform to increase their awareness about a particular topic or incident. Similarly, 73% of the respondents agreed that they share their knowledge to inform their colleagues/staff about new methods and software-related knowledge. 66% of the respondents share IS knowledge on the electronic platform to solve the problems of other members. 93% of the respondents participate in order to seek IS knowledge from the other members to solve the problems that they face in their professional tasks. 86% of the respondents apply the IS knowledge that they receive on the electronic platform to solve their problems.

Figure 12.6 presents that 96% of the respondents believe that it is essential for them to share their IS knowledge with other professionals in their field, and 96% of the respondents enjoy helping other professionals by sharing their IS knowledge. [mention controversy to lose competitive edge]. 72% of the respondents share their IS knowledge because it helps them achieve better results regarding the quality and productivity of the work in their projects. 57% of the respondents share their IS knowledge on the electronic communities because it helps in capturing and storing their knowledge so that it can be easily accessed and applied whenever they would

need it.

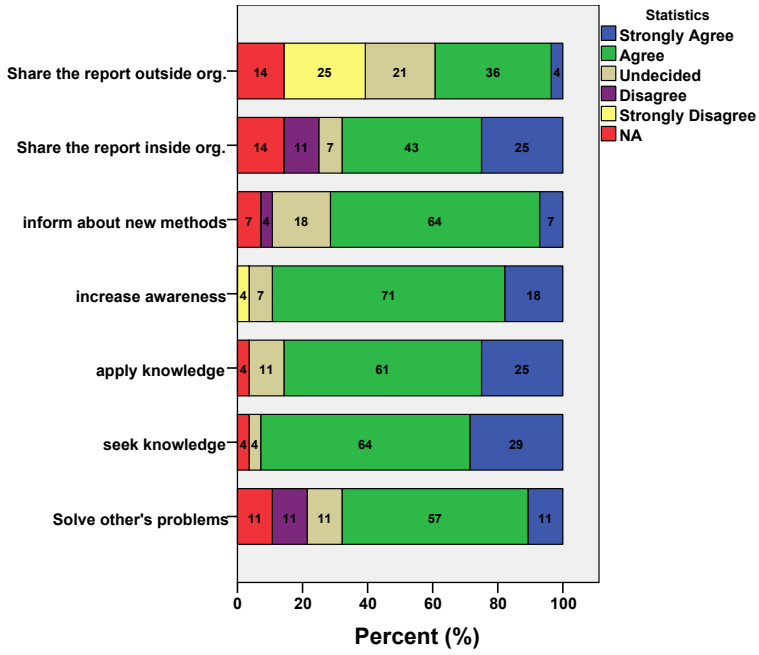


Figure 12.5: Factors that act as the main purpose of sharing IS knowledge on electronic platform

The factors related to extrinsic motivation is also analyzed in this study and presented in the figure 12.6. 85% of the respondents share their IS knowledge because it helps them to improve their reputation in the community of information security. 90% of the respondents agreed that share knowledge because it helps them to build relationships and network with other IS professionals. It is important for them to maintain a good relationship and be a part of the ISP network. The majority of the respondents are not so eager to gain an expert status as only 46% shares their knowledge to achieve this goal. The presence of any monetary benefits, i.e., reward, promotion, and salary hike do not motivate the respondents to share their knowledge as only 15% answered in favor of this factor.

12.5.3 Result III -Preference & Facilitating condition

Figure 12.7 presents the findings related to the preferences of the respondents during the participation and sharing of IS knowledge on eCoP. The preferences stated by the respondents define the features that they expect in the electronic platforms when they have to participate in knowledge sharing tasks. Only 25% of the respondents stated that they prefer to share their knowledge anonymously on elec-

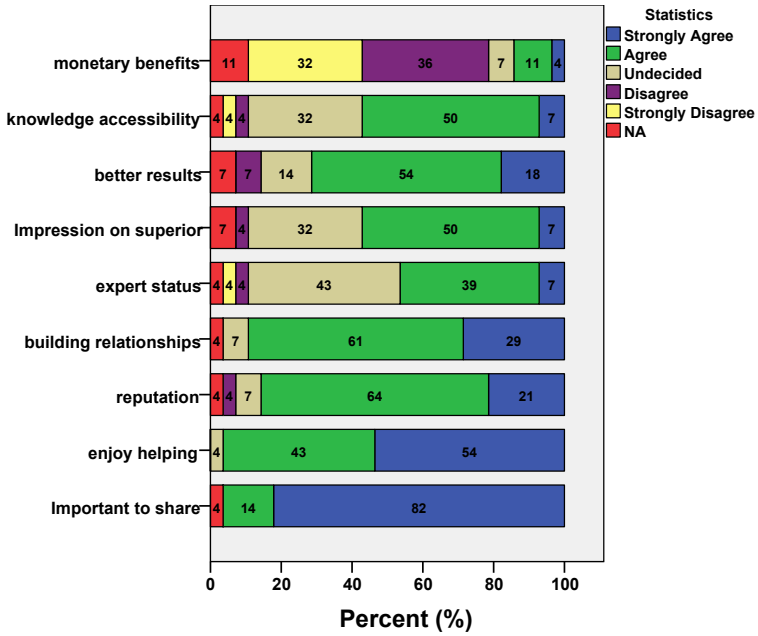


Figure 12.6: Factors act as a motivation to share IS knowledge

tronic platforms as they are concerned about their privacy. 18% of the respondents stated that share their knowledge only with the members whom they know personally. 32% of the respondents trust the content on eCoP only if it is validated by other IS professionals. 46% of the respondents trust the IS knowledge on eCoP only if they can see the true identity of the member who shared the information.

Figure 12.8 shows the findings to understand the importance of the facilitating conditions. 65% of the respondents agreed that they have enough training and skills to use electronic platforms to share their IS knowledge. 61% of the members agreed that their organization allows them to share their IS knowledge outside the organization, which means that the sharing of knowledge is not restricted to the closed community. 61% of the respondents do not face any problem sharing the IS knowledge on the electronic platform due to their current job role.

12.6 Discussion

The main objective of the present study is to identify the factors that are imperative in establishing UnRizkNow community. The primary purpose of any eCoP is to allow the members to share and access knowledge in the community. Therefore, UnRizkNow must support the provision of two-way knowledge exchange activity.

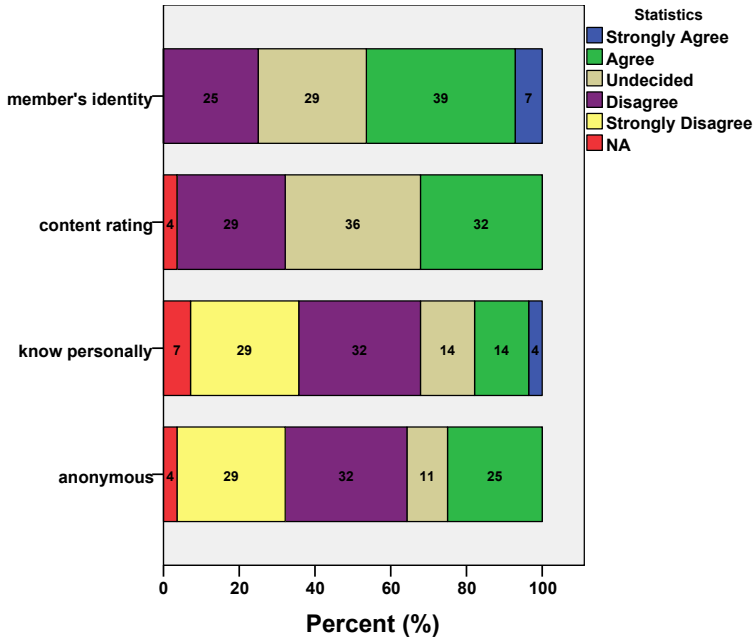


Figure 12.7: The preferences of the participants towards the features of eCoP

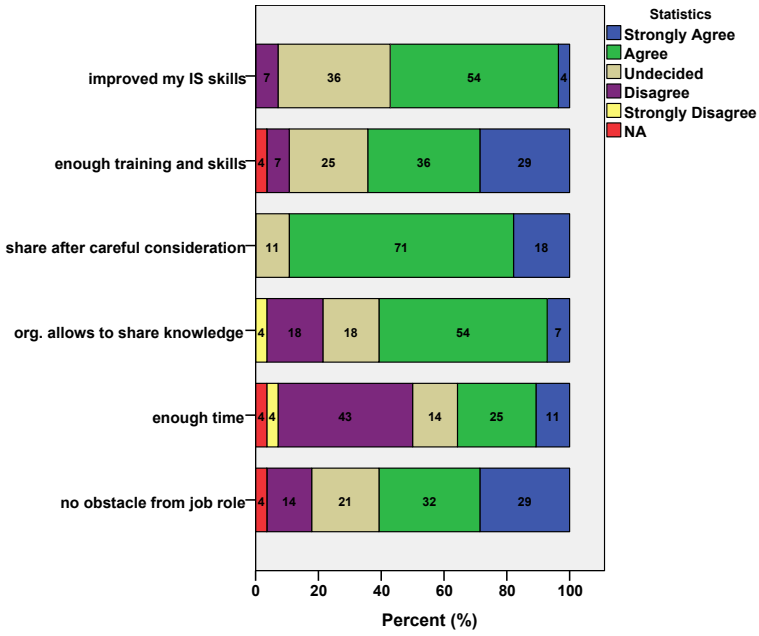


Figure 12.8: The facilitating condition to share IS knowledge

Hence, we started to develop UnRizkNow as a bulletin board that can be used to stay in touch with a group of people (community members). We adopted an open source software, phpBB [144] to power UnRizkNow community. phpBB enables the creation of forum dedicated to a particular topic with several features maintaining efficiency and ease of use. phpBB supports multiple database engines, but we selected MySQL for UnRizkNow. phpBB also supports user groups, attachment to the post, full-text search, private messaging, hierarchical subforums.

The primary aim of UnRizkNow is to provide solutions to the challenges faced by ISP in Norway. This can be achieved if the members share their knowledge with each other. UnRizkNow will serve as a platform where the members can share their knowledge using the capability provided by the online platform. In the context of the ISP maintaining and broadening their knowledge, skills, practice, and process of applying the knowledge gathered from others into routine practices, UnRizkNow aims to offer many essential services to the ISP. UnRizkNow provides knowledge sharing features such that the information accessible to ISP will experience an improvement in the following areas:

1. **Search:** The UnRizkNow platform must provide immediate or just-in-time access to a wide range of information in the community [127]. The survey results indicate that members prefer to share knowledge on the electronic platform to both learn and educate. It is therefore important that they must be able to search the content that they are looking for in the community. Figure 12.9 shows that we plugged-in both simple and advanced search feature in UnRizkNow platform. The simple search option allows to search for a 'word' or a 'sentence' in the database. However, the advanced search option enables the member to apply various in the search option. A member can select if the search operation is performed in the whole forum or selected subforum.

2. **Update:** Our survey result indicated that 93% of the respondents want to use the electronic platform to seek IS knowledge from the other members to solve their problems. The challenges/problems in IS domain require the latest mitigation strategy. Therefore, the UnRizkNow platform should allow the members to view the UpToDate information of the topics the members are interested. We addressed this requirement by including two features into UnRizkNow community. The added features are 'Recent topics' and 'subscribe topic.' The member can see the list of all the recent topics that are happening in the community. The member will get the list on the home page of the community. Additionally, a member can subscribe to a particular topic by selecting the option 'subscribe topic,' see Figure 12.10. The member will receive an e-mail when there is any information posted on the stated topic.

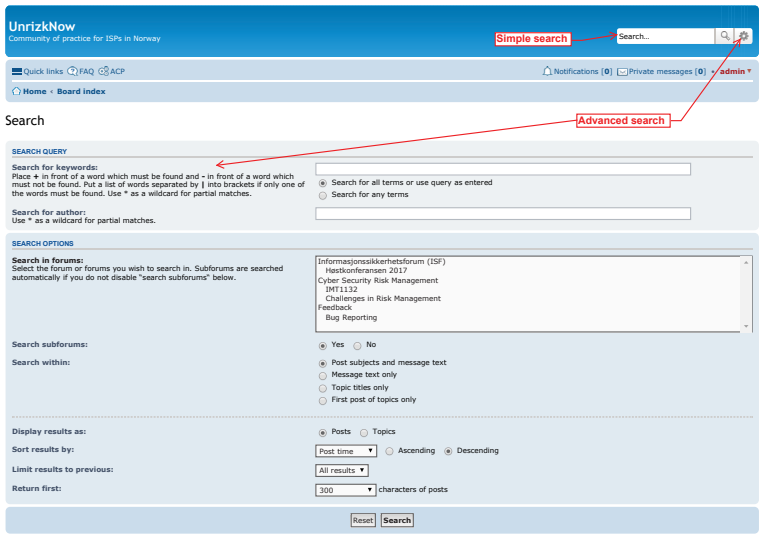


Figure 12.9: The search feature in UnRizkNow

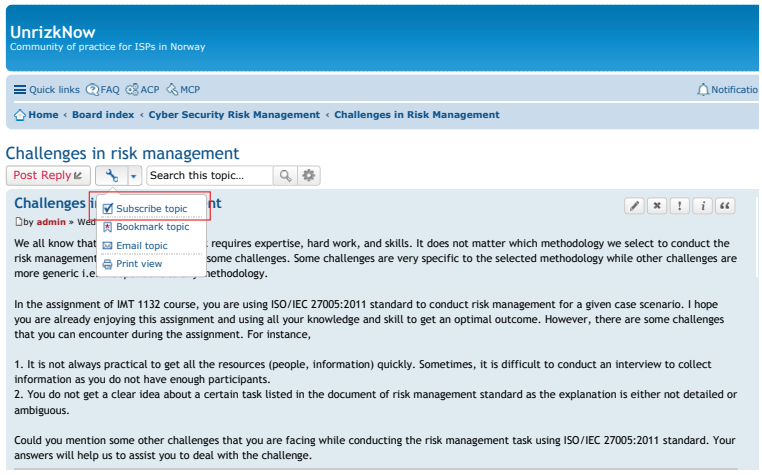


Figure 12.10: The update feature in UnRizkNow

3. **Reliance:** It is imperative for UnRizkNow community to provide information that the members that trust in it. It is also necessary that members can establish a good reputation in the community so that the content they provided can be trustworthy. Our survey states that 85% of the respondents want to establish a good reputation in the electronic community by sharing their knowledge. The members should be able to easily identify who are expert in the area and who is just the beginner. Therefore, we decided to introduce a reputation management system in the community. It allows the community members to rate posts or users, view rating statistics, reputation rankings.

Figure 12.11: The features in UnRizkNow that improve the trust

Figure 12.11 shows a snapshot of the reputation system details of the user 'test'. The current reputation of the user is 8. The reputation is calculated based on the following formula:

$$R = P_p + P_u$$

where R is reputation, P_p is the point for the posts, and P_u is the points obtained from the users. In the above scenario, the user 'test' received 2 points from two users for the post, and 6 points (5+1) from two users. In total, there are 4 positive ratings received by the user 'test'. Similarly, in the community, it will be possible to give positive or negative point to the post of a member.

The present setting of UnRizkNow does not allow the members to access the community anonymously. Members need to either select true identity or pseudonym (nicknames) to be eligible to post or read anything in the community. 61% of the members disagreed to share their knowledge anonymously. They believe that it is essential for them to use their identity while sharing.

4. **Importance:** The UnRizkNow platform must provide the features that are highly relevant to the ISP members regarding solving their challenges and meeting their needs. 68% of the members indicated that they share the report inside the organization to carry out their daily operation. Therefore, we added the feature to attach a file (any format) to share with the members through a post in the forum. The domain of the community is also well-defined and narrowed with the help of forum and subforum option. A person who is interested in a particular topic of Information security can browse the subforum of the community to find the relevant information. There is also an interesting feature added to acknowledge the relevant topic/post in the community. Figure 12.11 shows UnRizkNow community from the perspective of user 'test'. There is a post of the user 'vivek' in the community. User 'test' can see that the post of 'vivek' has already earned 1 point as someone gave a positive point to it. User 'test' can either provide a positive or negative point to the post of 'vivek' by selecting 'thumb up' or 'thumb down' symbols respectively.

5. **Structure:** UnRizkNow must act as a common platform for discussion and exchange ideas and resources to ensure the optimal solution for the information security challenges, unified and coordinated communication with the ISP [48]. 57% of the respondents agreed that they are willing to use an electronic platform to share knowledge if the platform helps in capturing and storing IS knowledge so that it could be easily accessed and applied whenever they need it. We added a feature to apply tag with the post so that all the post (information) can be collected at one place using the tag. For instance, if a member is interested to see all the posts related to 'security,' then the tagging feature will list all the posts that are marked with 'security.' Figure 12.12 shows different tag available in UnRizkNow community.

12.7 Research limitation and future work

The response that we received from 28 participants at ISACA workshop provided initial insight into understanding the different factors that are important to establish UnRizkNow. However, the findings cannot be generalized to a large population because of the small sample size. The future work will aim to recruit more ISP in Norway to participate in the online questionnaire. Furthermore, the sample is not

Figure 12.12: The tags used in UnRizkNow will be available on the home page

selected randomly in this study. The participants volunteered to participate in the online questionnaire. The choice of Likert scale (1-5) to collect response also gave us a minimal option to apply statistics. The future work will adopt a mechanism to design a continuous scale to collect data. The knowledge sharing features proposed in this study will be evaluated by ISP to understand the usefulness in the future study. The future work will also expand the research model by adding elements on security, and privacy concerning sharing knowledge in the community as well as using the knowledge outside the community.

12.8 Conclusion

In this study, we observed that ISP use electronic platform for both learning and educating. In other words, they want to share their knowledge with a purpose to solve the problems of other members as well as solve their own. The impact of intrinsic motivation is more than extrinsic motivation to encourage the members to participate actively. Members are not willing to exchange their knowledge anonymously, and rather they want to see the identity of the members whom they are exchanging their knowledge. Members also want to build their reputation in the community by participating in the community-based knowledge sharing activities. We proposed an online community of practice, UnRizkNow, that is developed based on the responses collected from the ISP affiliated with ISACA. We designed the features of the UnRizkNow such that the information accessible in the platform will help the members to search the information easily and quickly, get up-to-date information quickly, get more relevant content, establish reputation in the community, identify the members/post that is trustworthy, and get information in a

more collected way.

12.9 Acknowledgments

This study is a part of UnRizkNow project, which is funded by CCIS Norway. We would like to thank ISACA Norway for helping us gather the required data for the questionnaire and anonymous reviewers for their comments.

Chapter 13

Article 6: Secure Benchmarking Using Electronic Voting

Agrawal, Vivek; Snekkenes, Einar, Secure Benchmarking using Electronic Voting. In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT 2018, ISBN 978-989-758-319-3, pages 25-40.

13.1 Abstract

It is a common practice in the industry to organize benchmark processes to establish information security performance evaluation standards. A benchmarking system collects information security-related data from the organization to establish a standard. The information shared by the organization often contains sensitive data (details of the vulnerability, Cyber attacks). The present benchmarking systems do not provide a secure way of exchanging sensitive information between the submitter and the benchmark authority. Furthermore, there is a lack of any mechanism for the submitters to verify that the final benchmark result contains the response submitted by them. Hence, people are reluctant to take active participation in sharing their sensitive information in the benchmarking process. We propose a novel approach to solve the security limitations of present benchmarking systems by applying the concepts of electronic voting to benchmark. Our solution provides secrecy to the submitters' identity and secrecy to the benchmark responses. Our approach also ensures that all the submitted responses have been correctly counted and considered in the final benchmark result.

13.2 Introduction

Researchers and experts suggest that the development and use of sound and repeatable Information Security Management (ISM) practices bring organizations closer to meeting their business objectives. Organizations can measure the quality of ISM practices, either by comparing their processes to other organizations or by measuring compliance according to established security standards [193]. Information security is considered to be one of the business requirements that should be appropriately addressed by the enterprises. Enterprises hold a large volume of valuable information which is required to follow compliance with regulations and law about information security.

Benchmarking is a well-known process of improving performance by continuously identifying, understanding, and adapting security practices and processes found inside and outside an organization [76]. Benchmarking requires sharing organization-specific sensitive information to compare the performance in a specific domain. Typically, it requires Benchmark Submitters (members who possess valuable information) to submit the answers to a set of questions to establish a benchmark standard. However, the most significant barrier to benchmarking is the fact that many organizations are not willing to share their organization-specific sensitive data. The submitter may need to share the critical information, i.e., information related to security incidents that they often face. Information related to any successful attack is often perceived as a failure and is kept secret by the organization. The details of these events can create a bad image for the organization in the marketplace [193]. Any security incident within the company can jeopardize the business operation and reputation [102]. Therefore, it may be considered risky to participate in the benchmarking process as illegitimate access to the sensitive information may hamper the business operation of the organization.

Currently, benchmarking is practiced almost all over the world [138]. There is a variety of methods by which different forms of data are developed, collected, and transmitted during the benchmarking event. There may be conflicts of interests and incentives for the benchmark authorities to manipulate the benchmark process [88]. The current benchmarking models fail to provide a secure way to share sensitive information [102]. Benchmark does not provide an efficient way for the data submitters to verify that the final benchmark result contains the response submitted by them [4], [91]. Hence, it lacks the sense of transparency in collecting the data, analyzing the data, and publishing the final result.

We are establishing 'UnRizkNow' [15], [11], [6] as an open electronic community of practice (eCoP) [121], [194] to allow information security practitioners (ISP) to share InfoSec knowledge without violating the information security requirements.

We are working towards providing a secure benchmarking service on UnRizkNow eCoP. We aim to protect the identity of the members who participate in the benchmark task. We also target to protect the sensitive data shared by the members/organization in the benchmarking process. Therefore, we propose applying the concepts of electronic voting to the benchmarking process on eCoP. We formulate the current benchmarking model based on a literature review. We also establish the requirements of a secure benchmarking system. Furthermore, we map the benchmarking system to an electronic voting system by mapping their protocol, structure, and concepts. We also demonstrate how a secure benchmark can be conducted on the UnRizkNow platform using the electronic voting approach. We have identified the following research questions in this study.

RQ1 What are the requirements of a secure benchmarking system?
RQ2 How can a secure benchmarking system be mapped to an electronic voting system?
RQ3 How can a benchmarking system be built using the electronic voting concepts
RQ4 To what extent does the EV approach make the benchmarking system secure?

The paper is organized as follows: In Section 13.3, we overview of benchmarking and describe the benchmarking model that is widely used. In Section 13.4 the research method used in this study is described. In Section 13.5, an overview of the electronic voting system is presented. The essential phases of an EV system, the structure of vote, and security requirement of EV systems and schemes are also presented. A mapping of benchmarking concepts to EV concepts is presented in Section 13.6. In Section 13.7, an application of EV concepts to a benchmarking system is described to demonstrate how secure benchmarking can be conducted using the EV approach. A security analysis follows in Section 13.8. The limitation of the current study and the scope of further improvement is highlighted in Section 13.9. We conclude in Section 13.10.

13.3 Overview of benchmarking

This section aims to provide a general overview of benchmarking. We identify major activities and actors involved in a typical benchmarking system. The benchmark model that is widely used everywhere is also presented.

13.3.1 Benchmarking protocol

Development of benchmarks is an iterative and ongoing process that is likely to involve sharing information with other organizations working towards an agreeable

method [104]. Benchmarking is pioneered by Xerox Corporation in the 1979s to perform better in the international competition in the photocopier market [104]. The idea of benchmarking was restricted to very few companies, e.g., AT&T, Motorola, Xerox in the beginning. However, governmental and non-profit organizations have begun implementing benchmarking as late as the early 1990's. Information security Forum (ISF) provides benchmarks in the form of their premium service [91]. We derive the benchmarking protocol from the [53] report. A benchmarking system typically comprises the following activities and actors:

1. **Benchmark Administration**: It includes all the stages and processes involved in the benchmarking process. The establishment, design, production, and dissemination of a benchmark from the gathering of the input data and the calculation of the benchmark based on the input data to the dissemination of the Benchmark to users including any review, adjustment, and modification of this process. The legal person or entity responsible for executing this phase is called the *Benchmark Administrator* (BA). BA also takes care of publishing Benchmark values, which includes making available such values on the internet or by any other means, whether free of charge or not. According to [53] report, the activity of publishing benchmark values can be carried out by a separate entity, Benchmark Publisher.

2. **Benchmark Submission**: The activity of contributing to Benchmark data submissions to a BA. The Benchmark submission is done by *Benchmark Submitter* (BS). The data submitted by BS are used exclusively for the calculation of the Benchmark.

3. **Benchmark Calculation**: The activity of performing the calculation of the Benchmark based on the methodology provided by a Benchmark Administrator and the data collected by the entity performing the calculation or the BA or submitted by BS. A legal person or entity responsible for performing this phase is called *Benchmark Calculation Agent* (BCA).

4. **Benchmark service**: The activity of evaluating the performance in a certain domain by fetching benchmark data from BA. A profession client (by paragraphs 1, 2 and 3 of Section I of Annex II to Directive 2004/39/EC) who is interested in taking benchmark data from BA is called *Benchmark User* (BU).

The task of BA and BCA may be performed by distinct legal entities or may be grouped such that one entity performs more than one. Figure 13.1 shows the information flow among the actors involved in the benchmarking process.

13.3.2 Structure of a benchmark

The structure of the benchmark depends on the overall objective of the benchmark. A benchmark typically consists of some questions created to assess the performance of the various organization in a particular domain. The question has options which indicate the possible answer to the question. The structure containing the answers to the questions is called a response. There are the following types of question formats:

- Yes/No questions: Submitter's answer is either Yes or No. The benchmark result of this question is a histogram chart consists of the frequency distribution of yes and no generated from the valid responses.
- Multiple-option Question: A question consists of various options, but the submitter can submit only one option. The benchmark result of this question will be a histogram chart consists of the frequency distribution of all the options calculated from the valid response.
- Open question (Numerical): Submitter can formulate the answer and write it down. However, the answer must be a numeral that follows the condition provided in the question. For instance, the age of the submitter question can only take numbers in the range of 1-100. The benchmark result of this question will be an average value calculated on the total valid responses submitted by the benchmark submitter.

13.3.3 Benchmark model

In this study, the principles of benchmarking model are set up according to the guideline given by European Securities and Markets Authority (ESMA) and European Banking Authority [53]. The same principles are widely followed by many organizations, e.g., ISF [61], ABB [4] and ISM-Benchmark [102]. The benchmarking process is usually conducted in two phases, i.e., Benchmark standard establishment and Benchmark as a service. An overview of a complete benchmarking process is shown in Figure 13.1. The details of the two phases are given as follows:

13.3.3.1 Benchmark Standard Establishment

The first phase of the benchmark process is called Benchmark standard establishment. The aim of performing this phase is to collect data from the relevant organization to understand how well they perform in a given domain. This phase is usually executed synchronously, i.e., all the participants involved in the benchmarking task work simultaneously. Typically, BA hires or establishes a contract

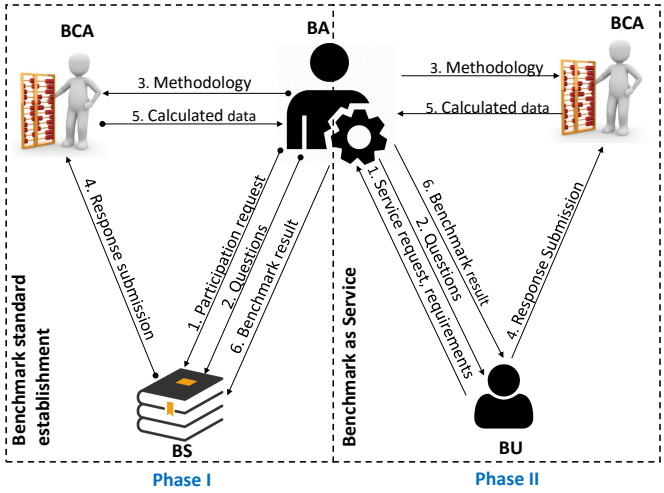


Figure 13.1: The information flow among the benchmarking actors in a benchmarking system. Phase I is carried out among BA, BCA, and BS. Phase II is carried out among BA, BCA, and BU

with an entity that can act as a BCA in the process. BA also makes a list of all the potential entities who can serve as a submitter. The details of step 1-6 in Phase I are given as follows:

1. BA sends a formal request to the members to participate in the benchmarking process and ask for response submission. The status of the member is marked as BS when the member agrees to participate
2. BA sends questions to assess a particular domain to BS.
3. BA sends the details of the question format and calculation method to BCA. The methodology is used by BCA to calculate the benchmark result.
4. BS sends the response to BCA.
5. BCA applies the methodology to the aggregated benchmark data and calculate the result of each question. BCA sends the benchmark result to BA.
6. BA sends the benchmark result to BS or posts it on a common web portal.

13.3.3.2 Benchmark as Service

The second phase of the benchmarking is called Benchmarking as a service. A private organization often provides it as a paid service, and by a public organization

(government) as a free service. A user (BU) who is interested to know the status of its performance usually go for this type of service. This phase is executed asynchronously, i.e., it is not necessary that all the users contact BA at the same time. However, there is some service-level-agreement involved between BA and BU. The details of the steps 1-6 in phase II are given as follows:

1. BU establishes a contract with BA to get the latest benchmarked data in the given domain. BU sends the details of the requirements, i.e., the domain of the benchmark, the format of the outcome, delivery time to BA.
2. BA chooses the relevant questions from the list used in phase I and creates a new set of questions specific to the requirement received from BU.
3. BA sends the details of the question format and calculation method to BCA. The methodology is used by BCA to calculate the benchmark result.
4. BU answers the questions of benchmark and sends the response to BCA.
5. BCA applies the methodology to the aggregated benchmark data from BU and calculate the result of each question. BCA sends the benchmark result to BA.
6. BA sends the benchmark result to BU. This benchmark result contains the response submitted by BU to the given questions and the values that have been collected by BA in phase I. In this way, BU can compare its response with the benchmark standard and assess its performance.

13.3.3.3 Requirements of a secure benchmarking system

In this section, we answer **RQ1** by establishing the security requirements of the benchmarking system. As far as we know, no comprehensive list of benchmarking security requirements have been published. Having carefully considered security issues in the context of benchmarking, we state what we believe are the key benchmarking security requirements.

1. **Completeness**: All valid responses should be counted correctly in the final calculation.
2. **Uniqueness**: Benchmark submitter can submit the response only once. The submitters should be allowed to submit their responses only once to control any practice to manipulate the overall result of the benchmark by submitting many responses.

3. **Universal verifiability**: Anyone can verify that the published result is correctly computed from the responses that were correctly submitted. This is an important requirement as it signifies that the benchmarked data is calculated using the originally submitted responses and it is not manipulated.

4. **Individual verifiability**: Each eligible submitter can verify that his valid response was counted.

5. **Eligibility**: Only entitled benchmark submitter can submit a response.

6. **Secrecy**: Neither benchmark authorities nor anyone else can find out which submitter submitted which response.

7. **Soundness**: Any invalid response should not be counted in the final calculation.

13.4 Research Method

We applied the concepts of Design Science Research (DSR) [75] to develop the scientific approach in this study. This research aims to solve an existing practical problem in the domain of Information system by creating an artifact based on the existing theories of electronic voting and cryptography. The problem is solved by applying creativity, innovation, and problem-solving capabilities. The created artifact would then be applied to UnRizkNow eCoP to enhance information sharing without compromising the sensitivity of the information. We adopted the five-step research process [96] to research this study. Figure 13.2 shows the essential steps in the DSR model.

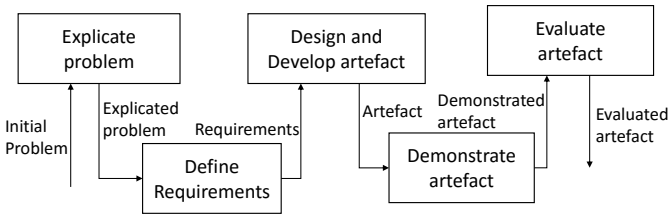


Figure 13.2: An overview of research method in Design Science Research Methodology [96]

The first step of the DSR process, i.e., *explicate problem* is to investigate and analyze the practical problem. We defined the problems in the present benchmarking system, i.e., the lack of security. Further, *define requirements* outlines a solution to the explicated problem in the form of an artifact and elicits requirements, which

can be seen as a transformation of the problem into demands on the proposed artifact. We suggest a novel approach of conducting benchmark using the concepts of the Electronic voting scheme. In the phase, *Design and develop artifact* an artifact is created to address the explicated problem and fulfill the defined requirements. Our artifact consists of mapping the structure, protocol, and the concepts of benchmarking to electronic voting. *Demonstrate artifact* uses the developed artifact and applies this to a real-life case or any illustrative case. This phase aims to show that the artifact can solve an instance of the defined problem. We incorporate the proposed artifact to the UnRizkNow platform so that a secure benchmarking can be conducted on the platform. The final step is *evaluate artifact*, which determines how well the designed artifact solves the primary problem. We perform the security analysis on the developed artifact to show to what extent it fulfills the security requirements of a secure benchmarking system.

We also applied the DSR knowledge contribution framework [67] to highlight the nature of the contribution of our study. Figure 13.3 presents a 2X2 matrix of DSR research contributions. The x-axis, i.e., Application Domain Maturity (ADM) shows the maturity of the problem from high to low. The y-axis, i.e., Solution Maturity (SM) represents the current maturity of the artifacts from high to low that exist as potential starting points for solutions to the questions. The 2x2 matrix also identifies four kinds of design science contribution. A low ADM and low SM defines a new solution for new problems, and it is referred to as *Invention*. A high ADM and Low SM define new solutions to known problems, also known as *Improvement*. A low ADM and High SM indicates known solutions for new problems, also known as *Exaptation*. Finally, A high ADM and high SM indicates known solution for known problems, referred to as *routine design*. Unlike other entities of the matrix, the routine design does not have a major knowledge contribution.

The idea of using the concepts of electronic voting conducting benchmarking tasks makes the benchmarking process more secure and trustworthy. The concept of electronic voting has been evolving in last two decades to facilitate election process in the democratic setting. However, it was never applied and tested in the setting of benchmarks. Therefore, our approach of solving the security and trust challenges in the present benchmarking process by extending the design knowledge that exists in the electronic voting place our contribution is in the ***exaptation*** quadrant of the DSR knowledge contribution framework.

13.5 An overview of electronic voting (EV)

The section aims to present a detailed description of the electronic voting protocol, the structure of electronic voting along with the security requirements.

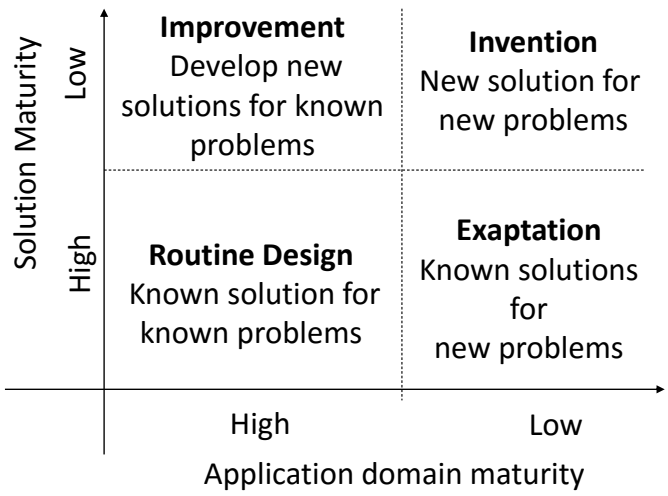


Figure 13.3: Design science contributions, adapted from [67]

13.5.1 Electronic Voting

Electronic voting (EV) is appearing as an efficient and cost-effective way of conducting a voting process. The term e-voting is used to denote a voting process which allows voters to cast a secure and secret ballot over a network [68]. The first EV scheme was proposed by David Chaum [38] in 1981. There have been many other schemes proposed by researchers since 1981, e.g., EV schemes with publicly verifiable secret sharing [159], [129]; EV based on homomorphic encryption [79]; EV based on secret sharing techniques with a secure multiparty computation [39]. [65] describes EV experiences by mentioning how EV systems worked in Geneva and Zurich in Switzerland. Similarly, the EV systems of Estonia are studied in [120], [182]. An EV protocol has many essential phases to carry out a successful election. We have compiled a list of phases that are very common across different EV protocols. The phases are as follows:

- Election administration: The process of setting up the election, publication of the identities of eligible voters, the list of candidates and the result of the election.
- Registration: The process of distributing secret credentials to voters and registering the corresponding public credentials.
- Tallying: The process of validating votes and determine the number of votes each party has received.
- Voting: The process of casting a vote in an election
- Ballot Processing: The processing of ballots and storing valid ballots in the

Table 13.1: Actors involved in EV process in different schemes

EV task	LE02 [112]	Belenios [43]	IVXV [137]	CHVote [72]	eVote [145]
Election administration	Election Administrator	Election Administrator	Organiser	Election Administrator	Managers
Registration	Certificate Authority	Registrar	Collector	Printing Authority, election authorities	Managers
Tallying	Tallier	Trustee	Tallier	Election Authorities	Managers
Ballot Processing	Tallier & Administrator	Bulletin Board Manager	Processor	Bulletin Board	Managers
Voting	Voter	Voter	Voter	Voter	Voter

bulletin board.

EV protocols involve several parties executing some specific set of roles [43]. However, different schemes use different terms to denote the parties involved in the EV process. Table 13.1 describes the actors who are responsible for performing the EV tasks in five EV schemes.

13.5.2 Structure of Electronic voting

The structure of voting depends on the nature of the election and the expected outcome. An election has a candidacy which consists of some candidates running in the election. A structure containing the vote is called a *ballot*. We identify the following typical election types:

- Yes/No voting: Voter's answer is yes or no. A typical example of this election where a voter is asked to reply to the question, "Do you agree with"regarding 'Yes' or 'No' answers.
- 1-out-of-L voting: Voter has L possibilities but can choose only one. This election format is used to select a leader (e.g., president) from a list of L candidates.
- K-out-of-L voting: Voter selects K different elements from the set of L possibilities. This type of election is used to choose council members in which the voter selects K from L candidates. The candidates who are selected the most number of times will be appointed as the council members. The order of the selection of the candidates is not important. $(1, L) \Rightarrow \{K \in \mathbb{N} : 1 \leq K \leq L\}$
- K-out-of-L ordered voting: Voter puts into order K different elements from the set of L possibilities. This type of election can be used to choose council

members, but the candidate who is marked by the voter as first will get the most points.

- Write-in Voting: Voter can formulate the answer and write it down. This type of election is done when the answers are not fixed at the beginning and voters are asked to give their opinion on the given matter.

13.5.3 Requirements of the secure electronic voting

Several researchers have proposed schemes for secure electronic voting processes with varying assumption. Therefore, different schemes fulfill different security requirements. We have compiled a list of requirements from different literature sources to highlight all the useful requirements that have been identified in the existing literature. We made a distinction between *schemes* and *systems* while compiling the list. Therefore, we have different criteria for the study selection in scheme and system.

Electronic voting scheme: Scheme is referred to the study where the conceptual model of electronic voting is presented regarding algorithm or theory. We used the search terms in Figure 13.4a to select the primary studies on the security requirements of electronic voting schemes. Additionally, we applied the following criteria on the search result to narrow down the relevant study.

- The literature is published on and after the year 2000.
- The literature has over 50 citations in the academic literature.
- Published in the English language.

The list is by far complete, but we restricted this study to include six schemes (Zu02 [156], Le02 [112], Le00 [111], Hi10 [78], Ch05 [37], Li04 [114].

Electronic voting system: We defined the system as those studies which are available as open source code, and it has been implemented in the real case studies. We used the search terms in Figure 13.4b to select the primary studies on the security requirements of the electronic voting system. Additionally, we applied the criteria that the source code is available to download on a reliable server (e.g., GitHub). English documentation or user manual also support the source code. The list is by far complete, but we restricted this study to include four electronic voting systems (eVote [145], Belenios [43], Chvote [72], IVXV [137]). The details of the requirements of EV protocol are as follows:

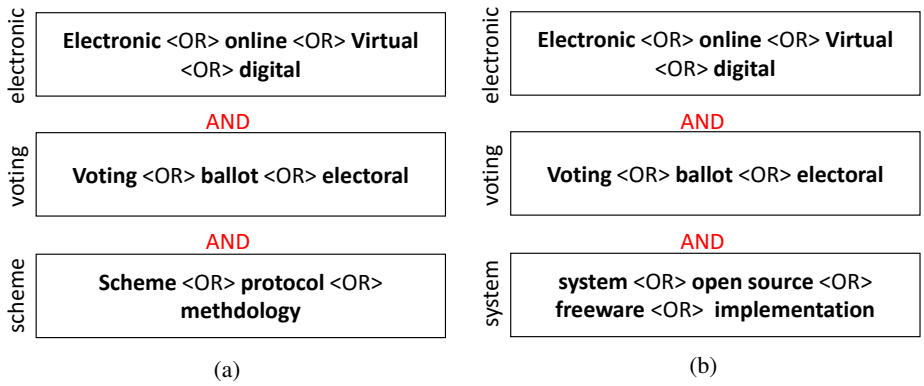


Figure 13.4: Search terms used to find a) Electronic voting scheme b) Electronic voting system

1. **Completeness/ Correctness**: All valid ballots should be counted correctly in the final tally [112], [78].

2. **Uniqueness/ Unreusability**: Voters can submit only one single ballot [78].

3. **Universal Verifiability**: Anyone can verify that the published tally is correctly computed from the ballots that were correctly cast [78], [156].

4. **Individual verifiability**: Each eligible voter can verify that his ballot was counted. This property enables the voter to exclude with high probability the possibility that a compromised voting client [72] has manipulated the vote.

5. **Eligibility**: Only entitled voters are able to cast a ballot [78].

6. **Anonymous/Secrecy/privacy**: Neither voting authorities nor anyone else can find out which voter submitted which ballot [114], [78].

7. **Soundness**: Any invalid ballot should not be counted in the final tally [78].

8. **Fairness**: No one can get extra information about the tally result before the publication phase [114].

9. **Receipt-freeness/Incoercibility**: The voter cannot be coerced into casting a particular vote by a coercer. He must neither obtain nor be able to construct a receipt proving the content of his vote [112], [114].

10. **Non-cheating**: Voters can accuse the authority of cheating without revealing ballots to others [114].

11. **Robustness**: The voting system should be successful regardless of the partial failure of the system [111].
12. **Convenience**: Voters to cast their ballots quickly, in one session, and with minimal equipment or special skills [114].
13. **Efficiency**: The whole election should be held promptly, for instance, all computations done in a reasonable amount of time and voters are not required to wait for other voters to complete the process [114].
14. **Mobility**: Voters are not restricted by physical location from which they can cast their votes [114].
15. **Auditability**: The system must be technically sufficiently simple so that a widest possible range of specialists could audit it [137].

Table 13.2 shows the list of the EV security requirements that are compiled from six EV schemes and four EV systems. The presence of **+** indicates that the given requirement is addressed. The requirement is considered as addressed if the author explicitly defines the given requirement in literature and justifies how the given EV protocol satisfies the requirement. **-** indicates that the given scheme/system does not address the requirement. It is also important to note that different schemes/systems address a security requirement under the different assumption and adversary models. For instance, the Hi10 [78] scheme addresses 'soundness' for K-out-of-L voting structure, and Zu02 scheme [156] addresses 'soundness' for 1-out-of-L voting structure. Similarly, the *uniqueness* requirement is addressed by LE02 [112] scheme under the assumption that an adversary cannot access the randomness and any internal information saved inside the tamper-resistant randomizer distributed to the voters. The Li04 scheme [114] addressed *uniqueness* requirement under the assumption that an adversary cannot obtain a random number generated by the voting center.

13.6 Mapping of a benchmarking to an EV system

This section aims to answer **RQ2**. We demonstrate how a benchmarking system can be mapped to the electronic voting system. To achieve our goal, we first map the benchmark protocol to the EV protocol, then we map the structure of the benchmark to the structure of the EV system. Finally, we map the overall concepts of the benchmark to the EV concepts using ontology.

13.6.1 Mapping of the benchmark protocol to EV protocol

The protocol mapping consists of the mapping of the benchmark phases and actors to the EV system phases and the actors. Table 13.3 shows the mapping of

Table 13.2: The security properties of EV system, AB: Applicability to Benchmark, **+** indicates that the given security requirement is implemented in the scheme, **-** indicates that the given security requirement is not implemented in the scheme.

ID	Property	AB	Zu02	Le02	Le00	Hi10	Ch05	Li04	Ch	Be	eV	IV
1	Completeness/ Correctness	Y	-	+	+	+	+	+	-	-	+	-
2	Uniqueness/ Unreusability	Y	-	+	+	+	-	+	-	-	+	+
3	Universal Verifiability	Y	+	+	+	+	-	-	+	+	+	-
4	Individual Verifiability	Y	+	+	-	+	-	+	+	+	+	+
5	Eligibility	Y	+	+	+	+	+	-	-	-	-	-
6	Anonymous/ Secrecy/privacy	Y	+	+	+	+	+	+	+	-	+	+
7	Soundness	Y	-	+	+	+	-	-	-	-	+	-
8	Fairness	N	+	+	+	+	-	+	-	-	+	-
9	Receipt-freeness/ Incoercibility	N	+	+	+	+	-	+	-	-	-	+
10	Non-cheating	N	-	-	-	-	-	+	-	-	+	-
11	Robustness	N	+	+	+	-	-	+	-	-	-	-
12	Convenience	N	-	-	-	-	-	+	-	-	-	-
13	Efficiency	N	-	-	-	-	-	+	-	-	-	-
14	Mobility	N	-	-	-	-	-	+	-	-	-	-
15	Auditability	N	-	-	-	-	+	-	+	-	-	+

benchmark protocol to EV protocol. The main entities involved in the benchmark protocol are: a Benchmark Administrator BA, N Benchmark Calculating Agents BCA_j ($j = 1, ..., N$), and M Benchmark submitter BS_i ($i = 1, ..., M$). The roles of each entity are as follows:

- Benchmark Administrator - BA verifies the identities and the eligibility of M submitters. BA manages the whole benchmarking process (creates questions and announces the benchmark result).
- Benchmark Submitter - There are M submitter BS_i ($i = 1, ..., M$). They have their digital signature keys certified by a certification authority (CA).
- Benchmark Calculating agent - There are N calculating agents BCA_j ($j = 1, ..., N$) who cooperatively decrypt the collected responses to open the result of benchmarking. A threshold t denotes the lower bound of the number of authorities that is guaranteed to remain honest during the protocol.

The main entities involved in the electronic voting protocol are: an Election administrator EA, N Tallier T_j ($j = 1, ..., N$), and M voter V_i ($i = 1, ..., M$). The roles of each entity are as follows:

- Election Administrator - EA verifies the identities and the eligibility of M voters. EA manages the whole voting process (creates candidacy and announces the election result).

Table 13.3: Mapping of the protocol

Phase		**Actor**	
Benchmark β	**EV** ω	**Benchmark** β	**EV** ω
Benchmark Administration $[BAdm]$	Election Administration $[EAdm]$	Benchmark Administrator $[BA]$	Election Administrator $[A]$
Benchmark calculation $[Bcal]$	Tallying $[ETal]$	Benchmark calculating agent $[BCA]$	Tallier $[T]$
Benchmark submission $[BSub]$	Voting $[Vo]$	Benchmark submitter $[BS]$, user $[BU]$	Voter $[V]$

- Voter - There are M voter V_i $(i = 1, ..., M)$. They have their digital signature keys certified by a certification authority (CA).
- Tallier - There are N Tallier T_j $(j = 1, ..., N)$ who cooperatively decrypt the collected ballots to open the result of the election. A threshold t denotes the lower bound of the number of authorities that is guaranteed to remain honest during the protocol.

Table 13.3 shows the mapping of the protocol between the benchmark and the EV system. It is clear from the table that the activity of Benchmark calculation can be mapped to Tallying, a benchmark submitter can be mapped to the voter.

13.6.2 Mapping of the benchmark structure to EV structure

We map the structure of the benchmarking system to an EV system with the help of the mapping of the ballot, vote, candidacy, and candidates to respond, answer, questions, and options respectively. Question QU is mapped to Candidacy Cd, Option o is mapped to Candidate C, answer a is mapped to vote v, response B is mapped to ballot BT. It is important to note that there is only one candidacy in an election, but a benchmark needs to have more than one question. Therefore, a benchmarking system needs the x number of EV instances to execute, where x is the number of questions in the benchmark.

In the electronic voting scheme ω, a candidacy Cd consists of L number of candidates C_i (where $i = 1, ..., L$) who participate in the election to be elected to some position based on the outcome of the election. A voter can decide to vote for only 1 candidate (1-out-of-L voting) or more than 1 candidate (K-out-of-L voting) based on the requirement of the election. A voter casts his ballot in the election. A

Table 13.4: Mapping of the benchmark structure to EV structure. There are M number of voters and submitters, x number of questions and candidacy, L number of option, answer, candidates, and votes

Benchmark					**EV**			
Question	Option	Answer	Response	$\Rightarrow$	Candidacy	Candidate	Vote	Ballot
Q_1	$o_1...o_L$	$a_1....a_L$	B_1		Cd_1	$c_1...c_L$	$v_1...v_L$	BT_1
Q_2	$o_1...o_L$	$a_1....a_L$	B_2		Cd_2	$c_1...c_L$	$v_1...v_L$	BT_2
...	...	...	...		...	...	...	...
...	...	...	...		...	...	...	...
Q_x	$o_1...o_L$	$a_1....a_L$	B_x		Cd_x	$c_1...c_L$	$v_1...v_L$	BT_x

ballot BT consists of a vector of votes, $\overrightarrow{v} = (v_1, ..., v_K)$, where v_i is the vote for the $i-$th candidate in the election. In K-out-of-L election, the following condition holds $(1, L) \Rightarrow \{K \in \mathbb{N} : 1 \leq K \leq L\}$.

A benchmarking system β consists of a number of questions Q_i (where $i = 1, ..., x$). The idea of having the questions is to collect the feedback from the submitters to establish a performance standard. Each question Q_i comes with the list of options o_i (where $i = 1, ..., L$). BS generates a vector of answers, $\overrightarrow{a} = (a_1, ..., a_L)$, where a_i is the answer of the $i-$th option and $a_i \in \{0, 1\}$. BS finally generates a response B consists of the answer vector $\overrightarrow{a}$. The number of response is equal to the number of questions available in the benchmark. The final response B_fin contains all the responses B_i $(i = 1, ..., x)$. Table 13.4 shows how the structure of the benchmark can be completely mapped to the structure of EV. The structure of benchmarking system can be constructed using the K-out-of-L voting structure where $(1, L) \Rightarrow \{K \in \mathbb{N} : 1 \leq K \leq L\}$. It is important to notice that 1-out-of-L voting structure is not suitable for the mapping between benchmark and electronic voting. 1-out-of-L voting structure expects only one vote in the ballot unlike K-out-of-L voting where a ballot contains a vector of votes. Therefore, BCA cannot calculate the frequency of individual option in the benchmark result using 1-out-of-L voting structure.

The structure of the benchmark for different question types are as follows:

13.6.2.1 Yes/No or True/False Questions

For this type of question in the benchmark $L = 2$, i.e., there are two options o_1 and o_2 available for the question. The answer vector will consist of $\overrightarrow{a} = (a_1, a_2)$. As submitter can select only option in the answer, the $\Sigma a_i = 1$. Therefore, the structure of $B = (a_1, a_2)$ The total response for this question is $M * B$ (where M is the number of submitters). The total number of *yes* can be counted by adding the a_1 answer vector and a total number of *No* can be counted by adding the a_2 answer vector from all the submitters.

$$\text{Result of } Q_j = \{\text{Frequency of } \textit{Yes} \text{ , Frequency of } \textit{No} \}$$
$$= \Sigma_{i=1}^{M} BS_i[B_j(a_1)], \Sigma_{i=1}^{M} BS_i[B_j(a_2)] \tag{13.1}$$

where $BS_i[B_j(a_1)]$ denotes the response B_J submitted by BS_i; $B_j(a_1)$ denotes the answer component a_1 of response B_j

This type of question in the benchmark is mapped to a K-out-of-L voting system (where $K = 1$) according to the mapping presented in Table 13.4. Yes, and No options are presented with candidate c_1 and c_2 respectively. The ballot BT contains the vote vector $\{v_1, v_2\}$ against the candidate c_1 and c_2. The frequency of yes and no can be counted by adding the votes cast by M voters in favor of the candidates. Equation 13.1 takes the following form in EV.

$$\text{result of } Cd_j = \{\text{votes received by } c_1 \text{ , votes received by } c_2 \}$$
$$= \Sigma_{i=1}^{M} V_i[BT_j(v_1)], \Sigma_{i=1}^{M} V_i[BT_j(v_2)] \tag{13.2}$$

where $V_i[BT_j(v_1)]$ denotes the ballot BT_J cast by V_i; $BT_j(v_1)$ denotes the vote component v_1 of Ballot BT_j

13.6.2.2 Multiple option Question

This type of question contains L possible option to choose from where $L > 2$. The answer vector will consist of $\overrightarrow{a} = (a_1, .., a_L)$. As submitter can select only one valid option out of L option, the $\Sigma a_i = 1$. Therefore, the structure of $B = (a_1, .., a_L)$ The total response for this question is $M * B$ (where M is the number of submitter). The frequency histogram can be generated by adding the answer vectors from all the submitters.

$$\text{Result of } Q_j = \{\text{Frequency of } o_1 \text{ ,...., Frequency of } o_L\}$$
$$\Sigma_{i=1}^{M} BS_i[B(a_1)], ..., \Sigma_{i=1}^{M} BS_i[B(a_L)] \tag{13.3}$$

where $BS_i[B_j(a_1)]$ denotes the response B_J submitted by BS_i; $B_j(a_1)$ denotes the answer component a_1 of response B_j

This type of question in benchmark is mapped to K-out-of-L voting system according to the mapping presented in Table 13.4. L possible options are mapped to L candidates. The ballot BT contains the vote vector $\{v_1, ..., v_L\}$ against the candidate $c_1, ...c_L$.The frequency of the $i-$th option is calculated by adding the

votes received to $i-$th candidate. Therefore, the equation 13.3 takes the following form in EV.

$$\Sigma_{i=1}^{M} V_i[BT_x(v_1)], ..., \Sigma_{i=1}^{M} V_i[BT_x(v_L)] \tag{13.4}$$

where $V_i[BT_j(v_1)]$ denotes the ballot BT_J cast by V_i; $BT_j(v_1)$ denotes the vote component v_1 of Ballot BT_j

13.6.2.3 Open Question (Numerical)

This type of question does not provide any pre-defined options to the submitters. However, the submitter can enter a numeric value in the options field. Option field consists of some empty bits based on the numerical range provided to the submitter. The value of L in the option field is calculated as the ceiling function of $log_2 MX$, i.e., $L = \lceil log_2 MX \rceil$ where MX is the range. The number entered by the submitter is converted into the equivalent binary string to be saved into the answer vector $\overrightarrow{a}$. Let's take the case of question 3 in the section 13.11, "*What percentage of the employee recognize a security issue? [range 0-100]*". The valid values this question takes is 101. Therefore, the value of L can be calculated by applying the ceiling function to $\lceil log_2 101 \rceil$, i.e., $L = 7$. Let's assume that BS submit 50 as the answer of the question. The answer vector $\overrightarrow{a} = (0100110)$. The total number of the response for question Q_j is $M * B$ (where M is the number of submitters). For option i (where $i = 1, ..., L$), the $i-$th components of each valid response of M submitters are summed up, i.e, $aa_i = \Sigma_{w=1}^{M} BS_w[B_j(a_i)]$, where aa_i is a count of the number of answers that has been received for the $i-$th bit of the binary representation to the question by all the submitters. The mean value of the Question Q_j is calculated by adding all aa_i in the following equation

$$\mu = \frac{1}{M} \Sigma_{i=1}^{L} aa_i 2^{i-1} \tag{13.5}$$

Open numerical question in benchmark is mapped to K-out-of-L voting system according to the mapping presented in Table 13.4. L possible options are mapped to L candidates. The ballot BT contains the vote vector $\{v_1, ..., v_L\}$ against the candidate $c_1, ...c_L$. The mean of the Question Q_x is calculated by firstly adding the $i-$th components of each valid ballot in vv, and then adding all vv and converting them to the decimal value. Equation 13.5 takes the following form:

$$vv_i = \Sigma_{w=1}^{M} V_w[BT_j(v_i)]; \mu = \frac{1}{M} \Sigma_{i=1}^{L} vv_i 2^{i-1} \tag{13.6}$$

where vv_i is a count of the number of votes that have been received for the $i-$th bit of the binary representation of the candidates to the candidacy by all the voters.

13.6.3 Mapping of overall concepts

We map the concepts of the benchmarking system to an electronic voting system using an ontology. The idea, of using and developing an ontology to explain the concepts, is derived from [9]. Figure 13.5 presents ontologies of the benchmarking system and electronic voting system. In our proposed ontology, there are ten main concepts (circular boxes) and ten relationships (solid arrow lines). The text above the horizontal dotted line corresponds to the benchmarking system, while the text below the horizontal dotted line corresponds to the electronic voting system. The dotted horizontal line also demonstrates how can a concept and relationship from benchmark be mapped to electronic voting. Thus, figure 13.5 helps to understand the relationship between the benchmark and electronic voting clearly. It is evident from the given ontology that the concepts of the benchmark can be mapped to the EV system.

The ontology of benchmark states that Benchmark Administrator performs benchmark administration by creating Benchmark. Benchmark has some Questions that consists of options. Submitter from different Organization participates in the Benchmark by submitting their response. A response contains an answer to the questions. A response can be considered valid or invalid on the basis of the benchmark rules. Benchmark calculating agent (BCA) counts response based on a given methodology, and finally, BA publishes the Benchmark result.

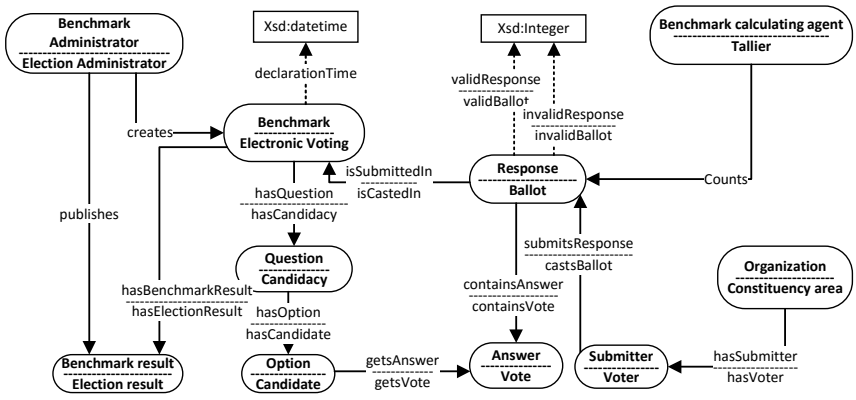


Figure 13.5: An ontology of benchmarking system and electronic voting system. The diagram shows that the concepts, actors, phases of benchmarking system can be mapped to electronic voting system.

The ontology also depicts that an election administrator (EA) performs administration by creating an election. The election has Candidacy that consists of some Candidate running for a certain post in the election. Voters from different Con-

stituency area participate in the election by submitting their ballot which contains the vote for the candidates. A ballot can be valid or invalid based on the election rule. A tallier collects and counts the valid ballot. EA finally declares the election result.

13.7 Secure benchmark on UnRizkNow

In this section, we answer our final research question **RQ3** by demonstrating the practical application of EV scheme to the benchmarking system using Hi10 scheme [78]. We present the model, set-up, response submission, benchmark calculation using the EV approach. This section aims to present how we can conduct a secure benchmark on **UnRizkNow** platform. The members of UnRizkNow are information security practitioners who possess knowledge about their organization regarding people, process, and technology. We use the cryptography tools mentioned in [78] to establish our model.

13.7.1 Preliminaries

$\Sigma-$**proofs**- A $\Sigma-$proof is a three-move special honest-verifier zero-knowledge proof of knowledge. A $\Sigma-$ proof is called *linear* if the verifier's test predicate is linear, i.e., the sum of two accepting conversations is accepting as well. The details of $\Sigma-$proof s is given in section 2.1 of [78]. BA acts as a verifier in our benchmark model.

Identification scheme - An identification scheme is an interactive protocol between two parties, a prover (benchmark submitter) and a verifier (Benchmark Administrator). If the protocol is successful, then at the end of the protocol the BA is convinced he is interacting with the BS, or more precisely, with someone who knows the secret key that corresponds to the prover's public key. For benchmark submitter identification, we assume an identification scheme where the identification protocol can be written as a linear $\Sigma-$proof . It is easy to verify that Schnorr's identification scheme [158] satisfies this requirement. The secret key of BS is denoted by z_v, and the corresponding public key by $Z_v = g^{z_v}$ for an appropriate generator g.

Designated-Verifier proofs- A designated-verifier proof is a proof which is convincing for one particular (designated) verifier, but completely useless when transferred from this designated verifier to any other entity [94]. The requirements of the encryption function are drawn from [78]. A semantically-secure probabilistic public-key encryption function $E_Z : \mathbb{V}X\mathbb{R} \Rightarrow \mathbb{E}, (a, \alpha) \mapsto e$, where Z denotes the public key, $\mathbb{V}$ denotes a set of answers, $\mathbb{R}$ denotes the set of random strings, and $\mathbb{E}$ denotes the set of encryptions. The decryption function is $D_z : \mathbb{E} \Rightarrow \mathbb{V}, e \mapsto a$, where z denotes the secret key. It is also required to have E to be $q-$ invertible

for a given $q \in \mathbb{Z}$. It implies that for every encryption e, the decryption a and the randomness α of qe can be efficiently computed. It is also required that there is a number $u \leqslant q$, large enough that $1/u$ is considered negligible [77]. Furthermore, we use modified ElGamal and Pailier homomorphic encryption function.

Moified ElGamal Encryption - A traditional ElGamal system with an encryption function E with the property: $E(M_1)XE(M_2) = E(M_1 + M_2)$.

Pailier Encryption - As mentioned in section 3.3 of [78].

Re-encrypting and proving Re-encryptions - A random re-encryption $e^{'}$ of a given encryption $e = E(a, \alpha)$ is an encryption with the same answer a, but a new (independently chosen) randomness $\alpha^{'}$. Such a re-encryption can be computed by adding a random encryption of 0 to e. The rest of the details can be obtained from [78] by substituting vote v with answer a, .

13.7.2 Details of the Benchmark protocol

We use the non-receipt free K-out-of-L voting protocol of [78] to establish our benchmark protocol. Figure 13.6 shows the various steps involved in carrying out the benchmark on UnRizkNow platform.

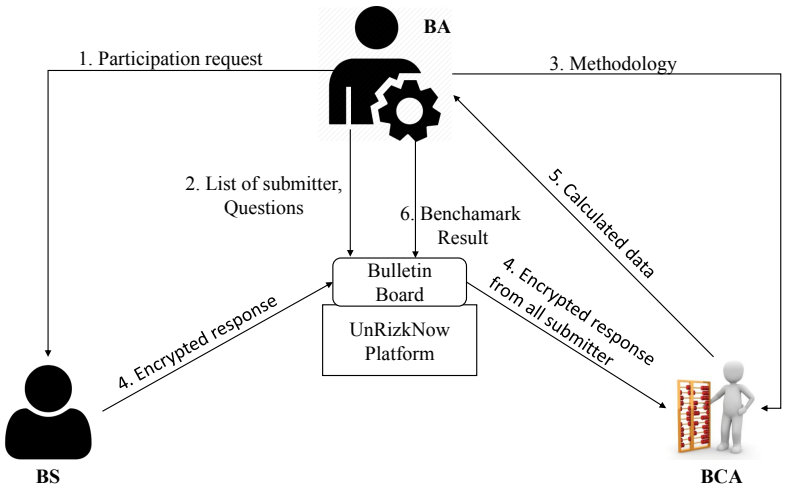


Figure 13.6: An overview of the benchmark model on UnRizkNow portal

Model - We use the benchmark entities as mentioned in the section 13.6.1. The communication among the benchmark entities happens through UnRizkNow platform. The platform has a bulletin board to post an announcement. BS post their encrypted response on the bulletin board with their signature. This also prevents re-submission of the responses on the bulletin board. Anyone can read and

verify the posted response on bulletin board, but nobody can delete the posted response. The bulletin board can be considered as an authenticated public channel with memory. The communication channel between BA and BS is secured using TLS. A threshold t denotes the lower bound of the number of authorities that is guaranteed to remain honest during the protocol.

Benchmark structure - The structure of question follows the structure mentioned in the section 13.3.2. We assume that we have yes/no, multiple choice, and open question (numerical) in the benchmark. A sample of the list of questions is given in Section 13.11. The mapping of the question to candidacy is performed as mentioned in the mapping section 13.6.2. The UnRizkNow platform maintains a double array $a[x][y]$ to save the label for the question format, and bit requires to generate the option for the question. The labels are yn for yes/no question, mc for multiple choice question, and op for the open numerical question. The submitter sees the questions in the form as presented in section 13.11. The platform has a program module m that reads the value from the array $a[x][y]$ and takes care of the translation of option o to the required bits.

Benchmark Administration - N calculating agents $(BCA_1, ...BCA_N)$ execute the key generation protocol using ElGamal encryption scheme. The resulting public key of the benchmarking system is announced to the registered members of UnRizkNow community, and the corresponding secret key is shared among BCA. BA also publishes the questions and response format on the bulletin board of UnRizkNow.

Benchmark submission - Benchmark submitter constructs a random encryption $\overrightarrow{e} = E(\overrightarrow{a}, \overrightarrow{\alpha})$ for his answer vector $\overrightarrow{a}$ and randomness $\overrightarrow{\alpha} \in_R \mathbb{R}^K$, and posts it onto the bulletin board of UnRizkNow. The submitter also posts a proof of validity. A response $B = \overrightarrow{a} = (a_1, ...a_K)$ is valid if and only if $a_i \in \{0, 1\}$ for $i = 1, ..., K$ and $\Sigma a_i = K$. A validity proof for the encrypted response $\overrightarrow{e} = (e_1, ..., e_K)$ is also constructed. The details of the construction of validity proof is given in section 5.4 in [78]. The encrypted response is submitted by BS to the bulletin board of UnRizkNow.

Benchmark calculation - BCA collects the encrypted responses from the bulletin board. The benchmark result Π is performed for each question separately. For Question Q_i, the $i-$th components of each valid encrypted response from M submitters are summed up using the homomorphic property of the encryption scheme and decrypted using the verifiable decryption protocol of the encryption scheme.

Benchmark result - The result of the benchmark is published for the individual questions. The result is calculated according to the equation 13.1, 13.3, 13.5.

13.8 Discussion

In this section, we answer the final research question **RQ4**. Firstly, we address the adversary model and the security assumption that we considered in this study. The adversary model highlights what the capabilities of an adversary are. Secondly, we perform the security analysis on the main security requirements which are typical for benchmarking systems. Finally, we mention the behavior of the benchmarking system using EV concepts towards the considered adversary model.

13.8.1 Adversary model and trust assumption

The adversary model depicts the attack potential that is a measure of the minimum effort to be expended in an attack to be successful [85]. The behavior of an adversary can change largely according to the implemented protocols and the capabilities of the adversary. A *internal* attacker is equipped with cryptographic keys and credentials that enable them to participate in the execution of the processes in the system. An *external* attacker does not possess such keys and credentials. In this section, we provide a general model of the adversary for the benchmarking system and EV system and map them.

In our adversary model, BS, BCA, and BA can act as an internal attacker to break the system secrecy, but not to influence the election outcome via bribery or coercion. We assume that all the parties involved in the benchmarking scenario are polynomially bounded and thus incapable of solving hard problems or breaking cryptographic primitives such as contemporary hash functions. Adversaries cannot efficiently decrypt ElGamal ciphertexts without knowing the private keys. For preparing and conducting a benchmark event, as well as for computing the final result, we assume that at least one honest benchmark authority does not collude. We take into the consideration that dishonest BCA may collude with the adversary, but not all of them in the same benchmark event. A threshold t denotes the number of BCA that is required to decrypt the responses, and which is also able to break the secrecy of an answer. BS cannot create an invalid response that can pass the validity proof. An external or internal adversary cannot delete any content from the UnRizkNow bulletin board.

13.8.2 Fulfillment of the security requirements of the benchmarking system

In this section, we show how the security requirements of the benchmarking system stated in section 13.3.3.3 can be fulfilled by adopting the EV approach. We establish the security of our proposed benchmark model using the established security proofs from the electronic voting scheme. We utilize the security proof and concepts given in [78].

1. **Completeness**: The dishonest submitter BS_i may create an invalid response, but the probability that the validity proof of encrypted response is negligible. Therefore, the invalidity of the encrypted response is detected in the validity proof of the scheme and the invalid vote will not be counted.

2. **Uniqueness**: The encrypted response along with the proof of the validity is posted on the bulletin board of UnRizkNow platform. Therefore, the submitter can submit only once, and the double submission is detected easily.

3. **Universal verifiability**: Anyone can read the encrypted response posted on the bulletin board. One can check its validity by verifying the K-out-of-L encryption proof. Since the encryption function uses the homomorphic property, he can also sum up all valid encrypted response to obtain the encryption of sum of the answers. Since the decryption is verifiable, he can also check whether the sum of the answers has been correctly decrypted [77], [78].

4. **Individual verifiability**: The individual verifiability of the benchmarking system is guaranteed by the homomorphic property of the encryption function and the verifiable decryption of the encryption scheme [77], [78].

5. **Eligibility**: The eligibility of the benchmarking system is ensured by the use of Schnorr's identification scheme. It is essential that each submitter know his secret key, and the public-key infrastructure ensures this. A protocol for ensuring knowledge of the secret key for Schnorr's identification scheme is provided in [79].

6. **Secrecy**: The secrecy of the benchmarking system is guaranteed under the assumption that no t BCA can maliciously pool their information and the assumption that the encryption scheme is semantically secure.

7. **Soundness**: The soundness of the benchmarking system can be proved using the proofs given in the re-encrypting and proving re-encryption of [78].

13.9 Limitation and Future work

The security requirements of the benchmarking system are formulated mainly to address the *secrecy* of the sensitive information shared by the benchmark submitter and the *transparency* of the benchmark process. There could be an extra requirement of receipt-freeness for an enhanced version of the benchmarking system. Receipt-freeness property ensures that the submitter cannot prove to a third party that they submitted a particular set of responses. The presence of this requirement avoids any selling of the data. A secure electronic voting scheme usually

addresses the receipt-freeness requirement because the selling of the vote is a serious problem in the election. The selling of the vote is often initiated by the entity who wants a certain candidate to win in the election. However, in our benchmark model, we do not think this problem is widespread as there is no candidate involved in it. However, the significance of this requirement needs further investigation by producing a use-case scenario.

The mapping of the benchmark structure to EV system uses K-out-of-L voting structure. We constructed a response as an answer vector $\overrightarrow{a}$ where $a_i \in \{0, 1\}$. The benchmark result is constructed by adding the $i-$th components of each valid response using the homomorphic property of the encryption function. Therefore, it is not possible to get the actual number entered by the submitter in the open numerical question as we cannot combine all the answers in the response and decrypt it. The system can apply homomorphic operation on the $i-$th bit of the answer. This property helps to ensure the confidentiality of the answer submitted, but at the same time, it does not allow to get all the actual numbers submitted by BS. The presence of an actual number in the benchmark could help to create a distribution graph of all the value submitted. Such a distribution graph would be more helpful as anyone could see the performance of all the submission and his submission. In other words, it would provide how many submission lies below and above his submission. However, in our proposed model, one can only see if his performance is either below or above the average performance.

Our proposed solution is still prone to a vulnerability of conflicts of interests in and incentives to manipulate the benchmark process where the benchmark submitters are also the market participants with stakes in the level of the benchmarks. The conflicts in the interest can create an incentive for abusive conduct of the benchmark process. Benchmark submitters may attempt to manipulate a benchmark by submitting false or misleading data to break the credibility of the benchmark result. Our future work will consist of conducting a risk analysis of the benchmarking system. We will adopt the CIRA method [6] to conduct the risk analysis exercise. This exercise will aim to assess the conflict in the interest of the stakeholders involved in the benchmarking system and propose the treatment plan to reduce the conflict.

The EV schemes and system that we analyzed in this study is far from the complete list. There might be more relevant EV schemes and system available that can be suitable for our benchmark model on UnRizkNow platform. As our future work, we would like to implement different electronic voting schemes on the UnRizkNow platform and test their performance in the benchmark context. We are also interested in conducting similar studies with Group Signature, the Secure Multi-Party computation to analyze their role in conducting secure benchmark on

UnRizkNow.

The ontology of benchmark and electronic voting presents an overview of the concepts and relationships involved in the system. The ontology needs to be formalized with Web Ontology Language (OWL) for modeling the ontology. The formal ontology will enable the possibility to be used by an automated tool to perform the mapping between benchmark and EV.

The future work also includes the assessment of other EV schemes to conduct secure benchmark on UnRizkNow. For instance, the LE02 schemes also meet all the requirements of the secure benchmark. Therefore, Le02 can also be a good candidate to adopt for a future secure benchmark solution. However, there is a concern with the efficiency of the LE02 scheme. This scheme has the overall performance complexity of $\mathcal{O}(xL^2B)$ where B represents the number of bits used to store one group element, x represents the number of questions, and L is the number of bits in the answer. In other words, every submitter sends his encrypted response using (xL^2B) bits. On the other hand, the overall performance complexity of Hi10 scheme is $\mathcal{O}(xLB)$. In other words, every submitter sends his encrypted response using the (xLB) bits.

13.10 Conclusion

We have presented the model of a benchmarking system that is typically used by an organization to establish the benchmark standard and provide the benchmark as a service. We highlighted the security challenges that the current benchmark model face, and therefore, a need to develop a more secure benchmarking system is also justified. The security limitation of current benchmarking systems may hinder the sharing of valuable information between the submitters and the benchmark authorities. Therefore, the requirements of a secure benchmarking system are established. We proposed a novel approach to solving the security limitation of benchmarking systems by adopting the secure cryptographic proofs from the field of secure electronic voting. We demonstrated how a benchmarking system could be mapped to the electronic voting system by mapping its protocol, structure, and concepts. We also demonstrated how the different formats of benchmark question can be presented and how the benchmark result can be calculated using the concepts of electronic voting. Our solution is based on the electronic voting protocol that provides secure transmission of the benchmark responses throughout the system. Furthermore, the identity of the response submitter is preserved by secrecy provided by the cryptographic protocols. The members who participate in the benchmark process can ensure that their responses have been counted correctly while calculating the benchmark result. Afterward, we demonstrated that how a secure benchmark can be designed for UnRizkNow platform using the concepts of

EV system. We showed that a benchmarking system is more secure if it follows the EV system approach as it can satisfy the necessary security requirements. We adopted Hi10 scheme to demonstrate the feasibility of our approach for UnRizkNow platform, but other relevant EV schemes can also be adapted to perform the benchmark on UnRizkNow platform.

13.11 List of Benchmarking Questions

1. Do you perform background checks on all employees with access to sensitive data, areas, or access points?
   - Yes
   - No
2. What percentage of the employee recognize a security issue? [range 0-100]
3. where do you store your sensitive information?
   - laptop
   - Paper document
   - Data server (internal)
   - Data Server (external)

Bibliography

[1] Class maxenttagger. http://www-nlp.stanford.edu/nlp/javadoc/javanlp/edu/stanford/nlp/tagger/maxent/MaxentTagger.html. Accessed: 2016-03-31.

[2] Stanford log-linear part-of-speech tagger. http://nlp.stanford.edu/software/tagger.html. Accessed: 2016-03-31.

[3] ISO/IEC GUIDE 73. Risk management - vocabulary . iso, 2009.

[4] ABB. Cyber security benchmark. http://new.abb.com/process-automation/process-automation-service/advanced-services/cyber-security-services/cyber-security-benchmark-and-fingerprint/cyber-security-benchmark1, 2017. Online; accessed 28 November 2017.

[5] V. Agrawal. A framework for the information classification in iso 27005 standard. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, pages 264–269, June 2017.

[6] V. Agrawal and A. Szekeres. Cira perspective on risks within unrizknow - a case study. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, pages 121–126, June 2017.

[7] Vivek Agrawal. A survey on information sharing practices. www.unrizk.org/survey/index.php/346746. Online; accessed 15 March 2017.

[8] Vivek Agrawal. Security and privacy issues in wireless sensor networks for healthcare. In Raffaele Giaffreda, Radu-Laurentiu Vieriu, Edna Pasher,

Gabriel Bendersky, Antonio J. Jara, Joel J.P.C. Rodrigues, Eliezer Dekel, and Benny Mandler, editors, *Internet of Things. User-Centric IoT*, pages 223–228, Cham, 2015. Springer International Publishing.

[9] Vivek Agrawal. Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, HAISA'16, pages 101–111, Frankfurt, Germany, 2016. Plymouth University.

[10] Vivek Agrawal. A comparative study on information security risk analysis methods. *Journal of Computers*, 12(1):57–67, 2017.

[11] Vivek Agrawal and Einar Arthur Snekkenes. *Factors Affecting the Willingness to Share Knowledge in the Communities of Practice*, pages 32–39. Springer International Publishing, Cham, 2017.

[12] Vivek Agrawal and Einar Arthur Snekkenes. An investigation of knowledge sharing behaviors of students on an online community of practice. In *Proceedings of the 5th International Conference on Information and Education Technology*, ICIET '17, pages 106–111, New York, NY, USA, 2017. ACM.

[13] Vivek Agrawal and Einar Arthur Snekkenes. Unrizknow: An open electronic community of practice for information security professionals. In *Proceedings of the 2017 9th International Conference on Education Technology and Computers*, ICETC 2017, pages 191–197, New York, NY, USA, 2017. ACM.

[14] Vivek Agrawal and Einar Arthur Snekkenes. Secure benchmarking using electronic voting. In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT,*, pages 25–40. INSTICC, SciTePress, 2018.

[15] Vivek Agrawal, Pankaj Wasnik, and Einar Arthur Snekkenes. Factors influencing the participation of information security professionals in electronic communities of practice. In *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, pages 50–60, 2017.

[16] Icek Ajzen. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179 – 211, 1991. Theories of Cognitive Self-Regulation.

[17] Maryam Alavi and Dorothy E. Leidner. Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, 25(1):107–136, 2001.

[18] Duane F. Alwin and Jon A. Krosnick. The measurement of values in surveys: A comparison of ratings and rankings. *The Public Opinion Quarterly*, 49(4):535–552, 1985.

[19] Ashton Anderson, Daniel Huttenlocher, Jon Kleinberg, and Jure Leskovec. Discovering value from community activity on focused question answering sites: A case study of stack overflow. In *Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '12, pages 850–858, New York, NY, USA, 2012. ACM.

[20] Alexander Ardichvili, Vaughn Page, and Tim Wentling. Virtual knowledge-sharing communities of practice at caterpillar: Success factors and barriers. *Performance Improvement Quarterly*, 15(3):94–113, 2002.

[21] Alexander Ardichvili, Vaughn Page, and Tim Wentling. Motivation and barriers to participation in virtual knowledge sharing communities of practice. *Journal of Knowledge Management*, 7(1):64–77, 03 2003.

[22] Alexandre Ardichvili, Martin Maurer, Wei Li, Tim Wentling, and Reed Stuedemann. Cultural influences on knowledge sharing through online communities of practice. *Journal of Knowledge Management*, 10(1):94–107, Jan 2006.

[23] P. Babcock. Shedding light on knowledge management. *HR Magazine*, 49(5):46–50, 2004.

[24] Timothy Barnett-Queen, Robert Blair, and Melissa Merrick. Student perspectives of online discussions: Strengths and weaknesses. *Journal of Technology in Human Services*, 23(3-4):229–244, 2005.

[25] Kathryn M. Bartol and Abhishek Srivastava. Encouraging knowledge sharing: The role of organizational reward systems. *Journal of Leadership & Organizational Studies*, 9(1):64–76, 2002.

[26] Colene Bentley, George P. Browman, and Barbara Poole. Conceptual and practical challenges for implementing the communities of practice model on a national scale - a canadian cancer control initiative. *BMC Health Services Research*, 10(1):3, 2010.

[27] Frank Blackler. Knowledge, knowledge work and organizations: An overview and interpretation. *Organization studies*, 16(6):1021–1046, 1995.

[28] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the 2001 Workshop on New Security Paradigms*, NSPW '01, pages 97–104, New York, NY, USA, 2001. ACM.

[29] Gee W. Bock and Young-Gul Kim. Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing. *Inf. Resour. Manage. J.*, 15(2):14–21, April 2002.

[30] Anne Bourhis, Line Dubé, Raal Jacob, et al. The success of virtual communities of practice: The leadership factor. *The Electronic Journal of Knowledge Management*, 3(1):23–34, 2005.

[31] John Seely Brown and Paul Duguid. Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. *Organization science*, 2(1):40–57, 1991.

[32] David Brownstone, David S. Bunch, and Kenneth Train. Joint mixed logit models of stated and revealed preferences for alternative-fuel vehicles. *Transportation Research Part B: Methodological*, 34(5):315 – 338, 2000.

[33] Angel Cabrera and Elizabeth F. Cabrera. Knowledge-sharing dilemmas. *Organization Studies*, 23(5):687–710, 2002.

[34] Angel Cabrera, William C Collins, and Jesus F Salgado. Determinants of individual engagement in knowledge sharing. *The International Journal of Human Resource Management*, 17(2):245–264, 2006.

[35] B.S. Chakravarthy, A. Zaheer, and S. Zaheer. *Knowledge Sharing in Organizations: A Field Study*. Discussion paper. Strategic Management Research Center, University of Minnesota, 1999.

[36] Elinor Ostrom Charlotte Hess. *Understanding Knowledge as a Commons: From Theory to Practice*. MIT Press, 2007.

[37] David Chaum, Peter Y. A. Ryan, and Steve Schneider. A practical voter-verifiable election scheme. In *Proceedings of the 10th European Conference on Research in Computer Security*, ESORICS'05, pages 118–139, Berlin, Heidelberg, 2005. Springer-Verlag.

[38] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90, February 1981.

[39] Chin-Ling Chen, Yu-Yi Chen, Jinn-Ke Jan, and Chih-Cheng Chen. A secure anonymous e-voting system based on discrete logarithm problem. *Applied Mathematics & Information Sciences*, 8(5):2571, 2014.

[40] Christy M.K. Cheung, Pui-Yee Chiu, and Matthew K.O. Lee. Online social networks: Why do students use facebook? *Computers in Human Behavior*, 27(4):1337 – 1343, 2011. Social and Humanistic Computing for the Knowledge Society.

[41] Peter Holdt Christensen. Knowledge sharing: moving away from the obsession with best practices. *Journal of Knowledge Management*, 11(1):36–47, 2007.

[42] Diane M. Christophel. The relationships among teacher immediacy behaviors, student motivation, and learning. *Communication Education*, 39(4):323–340, 1990.

[43] Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachène. *Election Verifiability for Helios under Weaker Trust Assumptions*, pages 327–344. Springer International Publishing, Cham, 2014.

[44] James Cox. Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5):1849 – 1858, 2012.

[45] John W Creswell. *Research design: Qualitative & quantitative approaches.* Sage Publications, Inc, 1994.

[46] Thomas H. Davenport and Laurence Prusak. *Information Ecology: Mastering the Information and Knowledge Environment*. Oxford University Press, 1st edition, 1997.

[47] Thomas H. Davenport, Lawrence Prusak, and Laurence Prusak. *Working Knowledge: How Organizations Manage What They Know*. Harvard Business School Press, Boston, MA, USA, 1997.

[48] George Demiris. The diffusion of virtual communities in health care: Concepts and challenges. *Patient Education and Counseling*, 62(2):178 – 188, 2006.

[49] Liping Deng and Nicole Judith Tavares. From moodle to facebook: Exploring students' motivation and experiences in online communities. *Computers & Education*, 68:167 – 176, 2013.

[50] R.T. Douglass, M. Little, and J.W. Smith. *Building Online Communities with Drupal, phpBB, and WordPress*. Expert's Voice in Open Source. Apress, 2006.

[51] M. Ehrig. *Ontology Alignment: Bridging the Semantic Gap*. Semantic Web and Beyond. Springer US, 2006.

[52] Richard M. Emerson. Social exchange theory. *Annual Review of Sociology*, 2:335–362, 1976.

[53] ESMA-EBA. Final report:esma-eba principles for benchmark-setting processes in the eu. Technical report, June 2013.

[54] Cath Everett. A risky business: {ISO} 31000 and 27005 unwrapped. *Computer Fraud & Security*, 2011(2):5 – 7, 2011.

[55] Daniel Feledi and Stefan Fenz. Challenges of web-based information security knowledge sharing. In *availability, reliability and security (ARES), 2012 seventh international conference on*, pages 514–521. IEEE, 2012.

[56] Daniel Feledi, Stefan Fenz, and Lukas Lechner. Towards web-based information security knowledge sharing. *Information Security Technical Report*, 17(4):199 – 209, 2013. Special Issue: ARES 2012 7th International Conference on Availability, Reliability and Security.

[57] S. Fenz, S. Parkin, and A. v. Moorsel. A community knowledge base for it security. *IT Professional*, 13(3):24–30, May 2011.

[58] Arlene Fink. *Conducting research literature reviews: from the Internet to paper*. Sage Publications, 2013.

[59] Waldo Rocha Flores, Egil Antonsen, and Mathias Ekstedt. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43:90 – 110, 2014.

[60] Michael A Fontaine and David R Millen. Understanding the benefits and impact of communities of practice. *Knowledge networks: Innovation through communities of practice*, pages 1–13, 2004.

[61] Information Security Forum. Benchmark as a service - information security forum. https://www.securityforum.org/products-services/benchmark-as-a-service/, 2017. Online; accessed 28 November 2017.

[62] Bruno S Frey and Margit Osterloh. *Successful management by motivation: Balancing intrinsic and extrinsic incentives*. Springer Science & Business Media, 2001.

[63] Marylène Gagné. A model of knowledge-sharing motivation. *Human Resource Management*, 48(4):571–589, 2009.

[64] D. Gefen, E. Karahanna, and D.W. Straub. Trust and tam in online shopping: An integrated model. *MIS Quarterly: Management Information Systems*, 27(1):51–90, 2003. cited By 2452.

[65] Jan Gerlach and Urs Gasser. Three case studies from switzerland: E-voting. *Berkman Center Research Publication No*, 3:2009, 2009.

[66] Asghar Ghasemi, Saleh Zahediasl, et al. Normality tests for statistical analysis: a guide for non-statisticians. *International journal of endocrinology and metabolism*, 10(2):486–489, 2012.

[67] Shirley Gregor and Alan R. Hevner. Positioning and presenting design science research for maximum impact. *MIS Q.*, 37(2):337–356, June 2013.

[68] Dimitris A Gritzalis. Principles and requirements for a secure e-voting system. *Comput. Secur.*, 21(6):539–556, October 2002.

[69] Thomas R. Gruber. Toward principles for the design of ontologies used for knowledge sharing. *Int. J. Hum.-Comput. Stud.*, 43(5-6):907–928, December 1995.

[70] Charlotte N. Gunawardena. Social presence theory and implications for interaction and collaborative learning in computer conferences. *International Journal of Educational Telecommunications*, 1(2):147–166, 1995.

[71] Ashish Gupta and Anil Dhami. Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice*, 17(1):43–53, 2015.

[72] Rolf Haenni, Reto E Koenig, Philipp Locher, and Eric Dubuis. Chvote system specification. *IACR Cryptology ePrint Archive*, 2017:325, 2017.

[73] Margaret C Harrell and Melissa A Bradley. Data collection methods. semi-structured interviews and focus groups. Technical report, Rand National Defense Research Inst santa monica ca, 2009.

[74] Alan Hevner and Samir Chatterjee. *Design research in information systems: theory and practice*, volume 22. Springer Science & Business Media, 2010.

[75] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Q.*, 28(1):75–105, March 2004.

[76] Antonio Hidalgo and Jose Albors. Innovation management techniques and tools: a review from theory and practice. *R&D Management*, 38(2):113–127, 2008.

[77] Martin Hirt. *Multi Party Computation: Efficient Protocols, General Adversaries, and Voting*. Hartung-Gorre, 2001.

[78] Martin Hirt. Towards trustworthy elections. chapter Receipt-free K-out-of-L Voting Based on Elgamal Encryption, pages 64–82. Springer-Verlag, Berlin, Heidelberg, 2010.

[79] Martin Hirt and Kazue Sako. *Efficient Receipt-Free Voting Based on Homomorphic Encryption*, pages 539–556. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[80] Kendall Ho, Sandra Jarvis-Selinger, Cameron D Norman, Linda C Li, Tunde Olatunbosun, Céline Cressman, and Anne Nguyen. Electronic communities of practice: guidelines from a project. *Journal of Continuing Education in the Health Professions*, 30(2):139–143, 2010.

[81] Peter Holdt Christensen. Knowledge sharing: Moving away from the obsession with best practices. *Journal of Knowledge Management*, 11(1):36–47, Feb 2007.

[82] George C. Homans. Social behavior as exchange. *American Journal of Sociology*, 63(6):597–606, 1958.

[83] Sherria L. Hoskins and Johanna C. Van Hooff. Motivation and ability: which students use online learning and what influence does it have on their achievement? *British Journal of Educational Technology*, 36(2):177–192, 2005.

[84] Meng-Hsiang Hsu, Teresa L. Ju, Chia-Hui Yen, and Chun-Ming Chang. Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *Int. J. Hum.-Comput. Stud.*, 65(2):153–169, February 2007.

[85] Muhammad Sabir Idrees, Yves Roudier, and Ludovic Apvrille. Model the System from Adversary Viewpoint: Threats Identification and Modeling. EPTCS 165, 2014, pp. 45-58, 2014. arXiv:1410.4305v1.

[86] Princely Ifinedo. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83 – 95, 2012.

[87] Innovation Insights. Using surveys for data collection in continuous improvement. *Office of planning and institutional assessment, The Penn State University, Innovation Insight Series*, 14:1–7, 2006.

[88] IOSCO. Principles for financial benchmarks. Technical report, July 2013.

[89] Minu Ipe. Knowledge sharing in organizations: A conceptual framework. *Human Resource Development Review*, 2(4):337–359, 2003.

[90] ISACA. Isaca norway chapter - sommermøte 2017, 2017.

[91] ISF. The isf benchmark and benchmark as a service. https://www.securityforum.org/tool/the-isf-benchmark-and-benchmark-as-a-service/, 2017. online; accessed 19 November 2017.

[92] Iso. ISO/IEC 27005 Information technology - Security Techniques - Information security risk management. Technical report, ISO, June 2008.

[93] Eric Iversen. Norwegian small and medium-sized enterprises and the intellectual property rights system: exploration and analysis, 2013.

[94] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pages 143–154, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[95] Suhwan Jeon, Young-Gul Kim, and Joon Koh. An integrative model for knowledge sharing in communities-of-practice. *Journal of Knowledge Management*, 15(2):251–269, 2011.

[96] Paul Johannesson and Erik Perjons. *An Introduction to Design Science*. Springer Publishing Company, Incorporated, 2014.

[97] Christopher M Johnson. A survey of current research on online communities of practice. *The Internet and Higher Education*, 4(1):45 – 60, 2001.

[98] Christopher M Johnson. Establishing an online community of practice for instructors of english as a foreign language. 2005.

[99] B.-S. Jong, C.-H. Lai, Y.-T. Hsia, T.-W. Lin, and Y.-S. Liao. An exploration of the potential educational value of facebook. *Computers in Human Behavior*, 32:201–211, 2014.

[100] R. Junco. Too much face and not enough books: The relationship between multiple indices of facebook use and academic performance. *Computers in Human Behavior*, 28(1):187–198, 2012. cited By 158.

[101] Pai Jung-Chi. An empirical study of the relationship between knowledge sharing and is/it strategic planning (issp). *Management Decision*, 44(1):105–122, 2006.

[102] Yasuko Kanno. Information security measures benchmark (ism-benchmark). Technical report, T Security Center, Information-technology Promotion Agency (IPA), 2009.

[103] Patricia Kearney, Timothy G. Plax, and Nancy J Wendt-Wasco. Teacher immediacy for affective learning in divergent college classes. *Communication Quarterly*, 33(1):61–74, 1985.

[104] Vassilis Kelessidis. Innoregio: dissemination of innovation management and knowledge techniques, 01 2000.

[105] Thomas Kemmerich, Vivek Agrawal, and Carsten Momsen. Chapter 10 - secure migration to the cloud-in and out. In Ryan Ko and Kim-Kwang Raymond Choo, editors, *The Cloud Security Ecosystem*, pages 205 – 230. Syngress, Boston, 2015.

[106] Dalkir Kimiz. Knowledge management in theory and practice. *McGill University*, 2005.

[107] Chakravanti Rajagopalachari Kothari. *Research methodology: Methods and techniques*. New Age International, 2004.

[108] Dragan Lambić. Correlation between facebook use for educational purposes and academic performance of students. *Computers in Human Behavior*, 61:313 – 320, 2016.

[109] Jean Lave and Etienne Wenger. *Situated learning: Legitimate peripheral participation*. Cambridge university press, 1991.

[110] Ryan Layfield, Murat Kantarcioglu, and Bhavani Thuraisingham. *Incentive and Trust Issues in Assured Information Sharing*, pages 113–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[111] Byoungcheon Lee and Kwangjo Kim. Receipt-free electronic voting through collaboration of voter and honest verifier. In *Proceeding of JW-ISC2000*, pages 101–108, 2000.

[112] Byoungcheon Lee and Kwangjo Kim. Receipt-free electronic voting scheme with a tamper-resistant randomizer. In *Proceedings of the 5th International Conference on Information Security and Cryptology*, ICISC'02, pages 389–406, Berlin, Heidelberg, 2003. Springer-Verlag.

[113] Daniel Z Levin, Rob Cross, Lisa C Abrams, and Eric L Lesser. Trust and knowledge sharing: A critical combination. *IBM Institute for Knowledge-Based Organizations*, 19, 2002.

[114] Horng-Twu Liaw. A secure electronic voting protocol for general elections. *Comput. Secur.*, 23(2):107–119, March 2004.

[115] Jeanne Liedtka. Linking competitive advantage with communities of practice. *Journal of Management Inquiry*, 8(1):5–16, 1999.

[116] Roderick JA Little. *Generalized Linear Models for Cross-classified Data from the WFS*. World Fertility Survey, International Statistical Institute, 1978.

[117] D. Liu, Y. Ji, and V. Mookerjee. Knowledge sharing and investment decisions in information security. *Decision Support Systems*, 52(1):95–107, 2011. cited By 20.

[118] Edwin A. Locke and Gary P. Latham. What should we do about motivation theory? six recommendations for the twenty-first century. *The Academy of Management Review*, 29(3):388–403, 2004.

[119] Soldal Lund, Folker den Braber, Ketil Stølen, Fredrik Vraalsen, Ida Solheim, and Mass Soldal Lund. A uml profile for the identification and analysis of security risks during structured brainstorming. 2004.

[120] Ülle Madise and Tarvi Martens. E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world. *Electronic voting*, 86(2006), 2006.

[121] Charla Mathwick, Caroline Wiertz, Ko de Ruyter, John Deighton served as editor, and Eric Arnould served as associate editor for this article. Social capital production in a virtual p3 community. *Journal of Consumer Research*, 34(6):832–849, 2008.

[122] Roger C. Mayer, James H. Davis, and F. David Schoorman. An integrative model of organizational trust. *The Academy of Management Review*, 20(3):709–734, 1995.

[123] J.P. Mazer, R.E. Murphy, and C.J. Simonds. I'll see you on "facebook": The effects of computer-mediated teacher self-disclosure on student motivation, affective learning, and classroom climate. *Communication Education*, 56(1):1–17, 2007. cited By 386.

[124] M. Mazzolini and S. Maddison. Sage, guide or ghost? the effect of instructor intervention on student participation in online discussion forums. *Computers and Education*, 40(3):237–253, 2003. cited By 160.

[125] Alan W McMorran. An introduction to iec 61970-301 & 61968-11: The common information model. *University of Strathclyde*, 93:124, 2007.

[126] David R. Millen, Michael A. Fontaine, and Michael J. Muller. Understanding the benefit and costs of communities of practice. *Commun. ACM*, 45(4):69–73, April 2002.

[127] P Nagy, CE Kahn Jr, W Boonn, K Siddiqui, C Meenan, N Knight, and N Safdar. Building virtual communities of practice. *Journal of the American College of Radiology: JACR*, 3(9):716, 2006.

[128] NaXa. Sensitive info disclosure. https://meta.stackoverflow.com/questions/338573/sensitive-info-disclosure, 2016. Online; accessed 15 March 2017.

[129] C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, CCS '01, pages 116–125, New York, NY, USA, 2001. ACM.

[130] W Lawrence Neuman. *Social research methods: Qualitative and quantitative approaches*. Pearson education, 2013.

[131] Van. Nguyen, Defence Science, and Technology Organisation (Australia). *Ontologies and information systems [electronic resource] : a literature survey / Van Nguyen*. Defence Science and Technology Organisation Edinburgh, S. Aust, 2011.

[132] Fred Nickols. Communities of practice. *A start-up kit*, 2003.

[133] I. Nonaka and H. Takeuchi. *The Knowledge-creating Company: How Japanese Companies Create the Dynamics of Innovation*. Everyman's library. Oxford University Press, 1995.

[134] Ikujiro Nonaka. A dynamic theory of organizational knowledge creation. *Organization Science*, 5(1):14–37, February 1994.

[135] Nicole Novielli, Fabio Calefato, and Filippo Lanubile. Towards discovering the role of emotions in stack overflow. In *Proceedings of the 6th International Workshop on Social Software Engineering*, SSE 2014, pages 33–36, New York, NY, USA, 2014. ACM.

[136] Natalya F. Noy and Deborah L. mcguinness. Ontology development 101: A guide to creating your first ontology. Online, 2001.

[137] State Electoral Office of Estonia. General framework of electronic voting and implementation thereof at national elections in estonia, June 2017.

[138] L. O'Rourke, National Research Council (U.S.). Transportation Research Board, National Cooperative Freight Research Program, United States. Department of Transportation. Research, and Innovative Technology Administration. *Handbook on Applying Environmental Benchmarking in Freight Transportation*. English short title catalogue Eighteenth Century collection. Transportation Research Board, 2012.

[139] Margit Osterloh and Bruno S. Frey. Motivation, knowledge transfer, and organizational forms. *Organization Science*, 11(5):538–550, 2000.

[140] Palych. Thanks for post. https://www.phpbb.com/customise/db/mod/thanks_for_posts. Accessed: 16.08.2016.

[141] Simon E. Parkin, Aad van Moorsel, and Robert Coles. An information security ontology incorporating human-behavioural implications. In *Proceedings of the 2Nd International Conference on Security of Information and Networks*, SIN '09, pages 46–55, New York, NY, USA, 2009. ACM.

[142] Suzanne D. Pawlowski, Dan Robey, and Arjan Raven. Supporting shared information systems: Boundary objects, communities, and brokering. In *Proceedings of the Twenty First International Conference on Information Systems*, ICIS '00, pages 329–338, Atlanta, GA, USA, 2000. Association for Information Systems.

[143] Teresa Susana Mendes Pereira and Henrique M. Dinis Santos. An ontology approach in designing security information systems to support organizational security risk knowledge. In *KEOD 2012 - Proceedings of the International Conference on Knowledge Engineering and Ontology Development, Barcelona, Spain, 4 - 7 October, 2012.*, pages 461–466, 2012.

[144] phpBB. phpbb #1; free and open source forum software. https://www.phpbb.com/, 2017.

[145] Massimo Di Pierro. evote tutorials, Dec 2017.

[146] Robert G. Powell and Barbara Harville. The effects of teacher immediacy and clarity on instructional outcomes: An intercultural assessment. *Communication Education*, 39(4):369–379, 1990.

[147] Nicolas Prat, Isabelle Comyn-Wattiau, and Jacky Akoka. Artifact evaluation in information systems design-science research-a holistic view. In *PACIS*, page 23. Citeseer, 2014.

[148] Gilbert Probst and Stefano Borzillo. Why communities of practice succeed and why they fail. *European Management Journal*, 26(5):335 – 347, 2008.

[149] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria, 2013. ISBN 3-900051-07-0.

[150] Lisa Rajbhandari and Einar Snekkenes. Risk acceptance and rejection for threat and opportunity risks in conflicting incentives risk analysis. In *International Conference on Trust, Privacy and Security in Digital Business*, pages 124–136. Springer, 2013.

[151] Lisa Rajbhandari and Einar Snekkenes. *Using the Conflicting Incentives Risk Analysis Method*, pages 315–329. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[152] Lisa Rajbhandari and Einar Arthur Snekkenes. Case study role play for risk analysis research and training. In *Proceedings of the 10th International Workshop on Security in Information Systems - Volume 1: WOSIS, (ICEIS 2013)*, pages 12–23, 2013.

[153] P. Rambe. Activity theory and technology mediated interaction: Cognitive scaffolding using question-based consultation on facebook. *Australasian Journal of Educational Technology*, 28(8):1333–1361, 2012. cited By 11.

[154] P. Ratnasingam. Trust in inter-organizational exchanges: A case study in business to business electronic commerce. *Decision Support Systems*, 39(3):525–544, 2005. cited By 87.

[155] Lawrence Vincent Redman and Austin Van Hoesen Mory. The romance of research. The Williams & Wilkins Company in coöperation with the Century of Progress Exposition, 1933.

[156] Zuzana Rjašková. Electronic voting schemes. *Diplomová práca, Bratislava*, 2002.

[157] Nader Sohrabi Safa and Rossouw Von Solms. An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57:442 – 451, 2016.

[158] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, Jan 1991.

[159] Berry Schoenmakers. *A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting*, pages 148–164. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[160] Arnhem Business school. Analysis multiple response categories. http://helpdeskspssabs.femplaza.nl/analysis/analysis_multiple_response_cat.htm. Accessed: 16.08.2016.

[161] Ulrike Schultze and Edwin L Cox. Investigating the contradictions in knowledge management. pages 155–174, 1998.

[162] Markus Schumacher. *6. Toward a Security Core Ontology*, pages 87–96. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[163] Sabine Seufert. The netacademy as a medium for learning communities. *Educational Technology & Society*, 3(3):122–136, 2000.

[164] Dong-Hee Shin. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interact. Comput.*, 22(5):428–438, September 2010.

[165] J. Short, E. Williams, and B. Christie. *The Social Psychology of Telecommunications*. Wiley, 1976.

[166] J. Short, E. Williams, and B. Christie. *The Social Psychology of Telecommunications*. Wiley, New York, 1976.

[167] Einar Snekkenes. Position paper: Privacy risk analysis is about understanding conflicting incentives. In *IFIP Working Conference on Policies and Research in Identity Management*, pages 100–103. Springer, 2013.

[168] Teodor Sommestad and Jonas Hallberg. A review of the theory of planned behaviour in the context of information security policy compliance. In Lech J. Janczewski, Henry B. Wolfe, and Sujeet Shenoi, editors, *Security and Privacy Protection in Information Processing Systems*, pages 257–271, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[169] Trent J. Spaulding. How can virtual communities create value for business? *Electronic Commerce Research and Applications*, 9(1):38 – 49, 2010. Special Issue: Social Networks and Web 2.0.

[170] Kurt D. Squire and Christine B. Johnson. Supporting distributed communities of practice with interactive television. *Educational Technology Research and Development*, 48(1):23–43, Mar 2000.

[171] S. Stefanov. *Building Online Communities with phpBB*. From technologies to solutions. Packt Publishing, Limited, 2005.

[172] Dick Stenmark. Leveraging tacit organizational knowledge. *J. Manage. Inf. Syst.*, 17(3):9–24, December 2000.

[173] Detmar Straub and Elena Karahanna. Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. *Organization Science*, 9(2):160–175, February 1998.

[174] SurveyMonkey. Learn how to conduct a survey | surveymonkey. https://www.surveymonkey.com/mp/how-to-conduct-surveys/?ut_source1=mp&ut_source2=survey_guidelines. (Accessed on 08/22/2018).

[175] Alireza Tamjidyamcholo, Mohd Sapiyan Bin Baba, Nor Liyana Mohd Shuib, and Vala Ali Rohani. Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, 43:19 – 34, 2014.

[176] Halbana Tarmizi and Gert Jan de Vreede. *A facilitation task taxonomy for communities of practice*, volume 7, pages 3532–3541. AMCIS 2005 Proceedings, 2005.

[177] Drew Tiene. Online discussions: A survey of advantages and disadvantages compared to face-to-face discussions. *J. Educ. Multimedia Hypermedia*, 9(4):371–384, January 2000.

[178] B. Tsoumas and D. Gritzalis. Towards an ontology-based security management. In *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06)*, volume 1, pages 985–992, April 2006.

[179] Abel Usoro, Mark W Sharratt, Eric Tsui, and Sandhya Shekhar. Trust as an antecedent to knowledge sharing in virtual communities of practice. *Knowledge Management Research & Practice*, 5(3):199–212, 2007.

[180] John Venable, Jan Pries-Heje, and Richard Baskerville. A comprehensive framework for evaluation in design science research. In Ken Peffers, Marcus Rothenberger, and Bill Kuechler, editors, *Design Science Research in Information Systems. Advances in Theory and Practice*, pages 423–438, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[181] Wesley C Vestal and Kimberly Lopez. Best practices: Developing communities that provide business value. In *Knowledge networks: Innovation through communities of practice*, pages 142–149. IGI Global, 2004.

[182] Priit Vinkel. *Internet Voting in Estonia*, pages 4–12. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[183] Agrawal Vivek. Community of practice for imt 1132. https://www.unrizk.org/, 2016.

[184] Agrawal Vivek. Community of practice for information security risk practitioners. https://www.unrizk.org/, 2016.

[185] Georg Von Krogh. Care in knowledge creation. *California management review*, 40(3):133–153, 1998.

[186] Artem Vorobiev, Nargiza Bekmamedova, et al. An ontology-driven approach applied to information security. *Journal of Research and Practice in Information Technology*, 42(1):61, 2010.

[187] Sheng Wang and Raymond A. Noe. Knowledge sharing: A review and directions for future research. *Human Resource Management Review*, 20(2):115 – 131, 2010.

[188] Gaute Wangen. Conflicting incentives risk analysis: A case study of the normative peer review process. *Administrative Sciences*, 5(3):125–147, 2015.

[189] M. McLure Wasko and S. Faraj. It is what one does: why people participate and help others in electronic communities of practice. *The Journal of Strategic Information Systems*, 9(2-3):155 – 173, 2000.

[190] Rolf H. Weber. Internet of things - need for a new legal environment? *Computer Law & Security Review*, 25(6):522 – 527, 2009.

[191] Etienne Wenger. *Communities of practice: Learning, meaning, and identity*. Cambridge university press, 1998.

[192] Etienne Wenger, Richard McDermott, and William Snyder. *Cultivating Communities of Practice: A Guide to Managing Knowledge*. Harvard Business School Press, Boston, MA, USA, 2002.

[193] Michael Whitman and Herbert Mattord. *Management of information security*. Cengage learning, 2014.

[194] Caroline Wiertz and Ko de Ruyter. Beyond the call of duty: Why customers contribute to firm-hosted commercial online communities. *Organization Studies*, 28(3):347–376, 2007.

[195] Kenneth Wong, Reggie Kwan, and Kat Leung. *An Exploration of Using Facebook to Build a Virtual Community of Practice*, pages 316–324. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[196] Ramazan Yilmaz. Knowledge sharing behaviors in e-learning community: Exploring the role of academic self-efficacy and sense of community. *Computers in Human Behavior*, 63:373 – 382, 2016.

[197] Pauline V Young and Calvin F Schmid. Scientific social surveys and research: An introduction to the background, content, methods, and analysis of social studies. 1939.

Part III

Appendix

Chapter 14

Appendix A

14.1 Java code to list the relevant terms of the domain

This section presents the java code that is used to compile the concepts and relationships in the ontology presented in the section 2.2. We captured terms that are important in describing the concept of ISO27005. It is a tedious task to go through the whole document (ISO27005 standard in this case) manually to capture all the relevant words. We may also fail to notice an important word if we scan the document manually. Therefore, we used an automated process to generate a list of all the relevant terms for ISO27005 standard. We used java API, MaxentTagger [1] to run, train, and test the part of speech (POS) tagger. We supplied the standard document of ISO27005 to the automated Process to extract all the distinct word from it. We tagged each word to its POS using English tagger *english-bidirectional-distsim.tagger* [2]. Later, we prepared a list of all nouns and verbs to select the relevant class entity, and relationship entity respectively. Some of the words contained in the list of noun includes - Risk, Asset, Event, Security incident, Threat, impact, likelihood, probability, consequence, control, mechanism, confidentiality, integrity, availability, objective, motive, media, organization, stakeholder, person, owner, industry, etc. Similarly, the words contained in the list of verb includes - mitigate, modify, cause, exploit, lead, affect, arise, become, begin, capture, allow, etc.

Listing 14.1: Java code to list the relevant terms

```
/*
 CC Coordinating conjunction
 CD Cardinal number
```

```
 DT Determiner
 EX Existential there
 FW Foreign word
 IN Preposition or subordinating conjunction
 JJ Adjective
 JJR Adjective, comparative
 JJS Adjective, superlative
 LS List item marker
 MD Modal
 NN Noun, singular or mass
 NNS Noun, plural
 NNP Proper noun, singular
 NNPS Proper noun, plural
 PDT Predeterminer
 POS Possessive ending
 PRP Personal pronoun
 PRP\$ Possessive pronoun
 RB Adverb
 RBR Adverb, comparative
 RBS Adverb, superlative
 RP Particle
 SYM Symbol
 TO to
 UH Interjection
 VB Verb, base form
 VBD Verb, past tense
 VBG Verb, gerund or present participle
 VBN Verb, past participle
 VBP Verb, non-3rd person singular present
 VBZ Verb, 3rd person singular present
 WDT Wh-determiner
 WP Wh-pronoun
 WP\$ Possessive wh-pronoun
 WRB Wh-adverb
 */
package dict;
import com.snowtide.PDF;
import com.snowtide.pdf.Document;
import com.snowtide.pdf.OutputTarget;
import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.DataInputStream;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
```

```
import java.io.IOException;
import java.io.InputStreamReader;
import java.io.OutputStreamWriter;
import java.io.Writer;
import java.util.ArrayList;
import java.util.List;
import java.util.StringTokenizer;
import edu.stanford.nlp.ling.Sentence;
import edu.stanford.nlp.ling.TaggedWord;
import edu.stanford.nlp.ling.HasWord;
import edu.stanford.nlp.tagger.maxent.MaxentTagger;
import java.io.FileReader;
import java.util.Collections;


public class Dict {
   static String pdfFilePath = "iso27005.pdf";
   Writer writer = null;
   static String pdfExtractFile = "PDFtext.txt";
   static String taggerFilePath =
      "english-bidirectional-distsim.tagger";
   static String distinctWordListFile =
      "DistinctWordList.txt";
   static String taggerListFile = "list_tag.txt";
   static String listOfPOSFile = "listOfPOS.txt";
   static String wordPOS = "VB"; //refer Part of speech
      list above

   public static void main(String[] args) throws
      java.io.IOException {
      Dict distFw = new Dict();

      try {
         //method call to extract text from a pdf file
         distFw.extractPDF();
         //method call to remove all the duplicates and
            'single letter word' from the file
         distFw.getDistinctWordList(pdfExtractFile);
         // method call to tag all the words with correct
            part of speech
         distFw.wordTag(taggerFilePath,
            distinctWordListFile);

         distFw.readPOS(taggerListFile);
      } catch (Exception ex) {
```

```
    }

}

/*
 This method reads the content of the .pdf file
    mentioned in the pdfFilePath variable
 and writes its content in a text file mentioned in the
    pdfExtractFile file.
 */
private void extractPDF() throws Exception {
   Document pdf = PDF.open(pdfFilePath);
   StringBuilder text = new StringBuilder(1024);
   pdf.pipe(new OutputTarget(text));

   // System.out.println(text);
   try {
      saveToFile(pdfExtractFile, text.toString());

   } catch (FileNotFoundException e) {
      System.err.println("Caught FileNotFoundException:
         " + e.getMessage());
   } finally {
      try {
         pdf.close();
      } catch (Exception ex) {
         System.err.println("Caught Exception: " +
            ex.getMessage());
      }
   }
}

/*
 This method Tags word written in the 'distinctfilename'
    with its corresponding part of speech using the
 tagger of 'taggerFilePath'.

 */
private void wordTag(String tagFile, String
    distinctfilename) throws Exception {

   List<TaggedWord> tSentence = null;
   try {
      MaxentTagger tagger = new MaxentTagger(tagFile);
      List<List<HasWord>> sentences =
```

```
            MaxentTagger.tokenizeText(new
            BufferedReader(new
            FileReader(distinctfilename)));
         for (List<HasWord> sentence : sentences) {
            tSentence = tagger.tagSentence(sentence);
            //System.out.println(Sentence.listToString(tSentence,
               false));
         }

         saveToFile(taggerListFile,
            Sentence.listToString(tSentence, false));
      } catch (FileNotFoundException e) {
         System.err.println("Caught FileNotFoundException:
            " + e.getMessage());
      }
   }

   /*
    This is a method to remove all the duplicates from a
       text file. It creates a txt file with
    a list of all the unique words in a given file. It also
       removes alphabets from the file.
    */
   private void getDistinctWordList(String fileName)
      throws Exception {
      FileInputStream fis = null;
      DataInputStream dis = null;
      BufferedReader br = null;
      boolean check = true;
      List<String> wordList = new ArrayList<String>();
      try {
         fis = new FileInputStream(fileName);
         dis = new DataInputStream(fis);
         br = new BufferedReader(new
            InputStreamReader(dis));

         String line = null;
         while ((line = br.readLine()) != null) {
            StringTokenizer st = new StringTokenizer(line,
               " ,.;:\"()-/[]");

            while (st.hasMoreTokens()) {
               String tmp = st.nextToken().toLowerCase();
               tmp = tmp.replaceAll("[^a-z]", "");
               if (tmp.length() > 2) {
```

```
                check = checkDictionary(tmp);
                if (!wordList.contains(tmp) && check ==
                    true) {
                   wordList.add(tmp);

                }

             }
          }
       }
       Collections.sort(wordList);
       saveToFile(distinctWordListFile,
          wordList.toString());
    } catch (FileNotFoundException e) {
       System.err.println("Caught FileNotFoundException:
          " + e.getMessage());
    } catch (IOException e) {
       System.err.println("Caught IOException: " +
          e.getMessage());
    } finally {
       try {

          if (br != null) {
             br.close();
          }
       } catch (Exception ex) {
          System.err.println("Caught Exception: " +
             ex.getMessage());
       }
    }
}

private boolean checkDictionary(String word) throws
    Exception {
   FileInputStream fis = null;
   DataInputStream dis = null;
   BufferedReader br = null;
   try {
      fis = new FileInputStream("lib\\wordsEn.txt");
      dis = new DataInputStream(fis);
      br = new BufferedReader(new
         InputStreamReader(dis));
      String line = null;
      while ((line = br.readLine()) != null) {
```

```
            if (line.contains(word)) {
               return true;
            }
         }
      } catch (FileNotFoundException e) {
         System.err.println("Caught FileNotFoundException:
            " + e.getMessage());
      } finally {
         try {
            if (br != null) {
               br.close();
            }
         } catch (Exception ex) {
            System.err.println("Caught Exception: " +
               ex.getMessage());
         }
      }
      return false;
   }

   /*
    Method to read a particular POS from a tagged file.
    */
   private void readPOS(String fileName) throws Exception {

      FileInputStream fis = null;
      DataInputStream dis = null;
      BufferedReader br = null;
      List<String> wordList = new ArrayList<String>();
      try {
         fis = new FileInputStream(fileName);
         dis = new DataInputStream(fis);
         br = new BufferedReader(new
            InputStreamReader(dis));
         String line = null;
         while ((line = br.readLine()) != null) {
            StringTokenizer st = new StringTokenizer(line,
               " ");
            while (st.hasMoreTokens()) {
               String tmp = st.nextToken().toUpperCase();
               int k = tmp.indexOf(wordPOS);
               int z = tmp.length();
               if (z > 1 & k > 0) {
                  tmp = tmp.substring(0, k - 1);
                  tmp = tmp.replaceAll("[^A-Z/,]", "");
```

```
                    System.out.println(tmp);
                    if (!wordList.contains(tmp)) {
                       wordList.add("\n"+ tmp);
                    }
                 }
              }
           }
           Collections.sort(wordList);
           saveToFile(listOfPOSFile, wordList.toString());
        } catch (FileNotFoundException e) {
           System.err.println("Caught FileNotFoundException:
              " + e.getMessage());
        } finally {
           try {
              if (br != null) {
                 br.close();
              }
           } catch (Exception ex) {
              System.err.println("Caught Exception: " +
                 ex.getMessage());
           }
        }
     }

     private void saveToFile(String filename, String
        content) throws Exception {
        try {
           writer = new BufferedWriter(new
              OutputStreamWriter(
                 new FileOutputStream(filename), "utf-8"));
           writer.write(content);
        } catch (IOException ex) {
           System.err.println("Caught IOException: " +
              ex.getMessage());
        } finally {
           try {
              writer.close();
           } catch (Exception ex) {/*ignore*/

              System.err.println("Caught Exception: " +
                 ex.getMessage());
           }
        }
     }
}
```

14.2 Automated code to stress test survey tool

This section presents a code snippet to perform stress test of the online questionnaire used in the Article 2-5. This code is helpful to test if the server and database can handle the concurrent request of the respondents. As we used LimeSurvey tool and private domain to host our questionnaire, this exercise proved to be very helpful in the study. This code also generates a sample data for the survey according to the desired participants (invocation count). In the following code, invocation count defines the total number of participants who are participating in the survey, and threadPoolSize defines the number of respondents who can access the questionnaire simultaneously.

```
package test;

import org.testng.annotations.Test;

import java.util.concurrent.TimeUnit;

import org.openqa.selenium.By;
import org.openqa.selenium.WebDriver;
import org.openqa.selenium.WebElement;
import org.openqa.selenium.chrome.ChromeDriver;



public class stressTest {

   @Test(invocationCount =200, threadPoolSize =50)
   public void testing() {
      // TODO Auto-generated method stub
      //System.setProperty("webdriver.firefox.marionette",
      "E:/Stress Test/geckodriver.exe");
      //WebDriver driver = new FirefoxDriver();

      //First Page
      System.setProperty("webdriver.chrome.driver",
      "E:/Stress Test/chromedriver.exe");
      WebDriver driver = new ChromeDriver();
      driver.get("https://www.unrizk.org/survey/index.php/342948");
      driver.findElement(By.xpath("//button[@value='movenext']"))
      .click();

      //Second page
      //driver.manage().timeouts().implicitlyWait(2,
```

```
    TimeUnit.SECONDS);
driver.findElement(By.cssSelector("[name='342948X1X1']
[id='answer342948X1X1A3'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X1X2']
[id='answer342948X1X2A5'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X1X3']
[id='answer342948X1X3A3'][type='radio']")).click();
driver.findElement(By.xpath("//button[@id='movenextbtn']"))
.click();


//Third page
//driver.manage().timeouts().implicitlyWait(2,
    TimeUnit.SECONDS);
//driver.findElement(By.cssSelector("[name='342948X2X4']
[id='answer342948X2X4A2'][type='radio']")).click();

driver.findElement(By.cssSelector("[name='342948X2X5SQ001']
[id='answer342948X2X5SQ001-A2'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X2X5SQ002']
[id='answer342948X2X5SQ002-A2'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X2X5SQ003']
[id='answer342948X2X5SQ003-A2'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X2X5SQ004']
[id='answer342948X2X5SQ004-A2'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X2X5SQ005']
[id='answer342948X2X5SQ005-A2'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X2X5SQ006']
[id='answer342948X2X5SQ006-A2'][type='radio']")).click();
driver.findElement(By.cssSelector("[name='342948X2X5SQ007']
[id='answer342948X2X5SQ007-A2'][type='radio']")).click();

//driver.findElement(By.id("answer342948X2X6")).sendKeys("random");

//WebElement element =
    driver.findElement(By.id("answer342948X2X6"));
//element.click();
//element.clear();
//element.sendKeys("Vivek Agrawal");

driver.findElement(By.cssSelector("[name='342948X2X7SQ001']
[id='answer342948X2X7SQ001-A2'][type='radio']")).click();

driver.findElement(By.cssSelector("[name='342948X2X7SQ002']
[id='answer342948X2X7SQ002-A3'][type='radio']")).click();
```

```
    driver.findElement(By.xpath("//button[@id='movenextbtn']"))
    .click();

    //4thg page

    driver.findElement(By.cssSelector("[name='342948X3X16']
    [id='answer342948X3X16A2'][type='radio']")).click();

    driver.findElement(By.xpath("//button[@id='movenextbtn']"))
    .click();

    driver.findElement(By.xpath("//button[@id='movesubmitbtn']"))
    .click();

    driver.manage().timeouts().implicitlyWait(10,
        TimeUnit.SECONDS);


    }

}
```

Chapter 15

Appendix B

15.1 Questionnaire 1: UnrizkNow and knowledge sharing

This section presents the list of questions used to collect data in chapter 8.

1. Which group were you a member of? * *Select only one option*

○ Riskorg (Group 1), ○ Soteria (Group 2), ○ Baeblade (Group 3), ○ Fredrik's Minions (Group 4)

2. How much experience did you have working with formal risk and vulnerability analysis before you are admitted to IMT 1132? * *Select only one option*

○ No experience, ○ Basic experience (1-3 risk assessments previously), ○ Medium experience (4-10), ○ High experience (over 10), ○ Other:

3. How much time (average) did you spend working on IMT 1132 per week? * *Select only one option*

○ 0-3 hours, ○ 4-7 hours, ○ 8-14 hours, ○ more than 15 hours

4. How useful was UnRizkNow platform to solve your project? * *Select only one option per row*

	Low	Medium	High
For Learning	○	○	○
For sharing information	○	○	○
Q&A with the instructor	○	○	○

5. Although knowledge sharing has many advantages, it was only moderate traffic on UnRizkNow. What do you think was the main reason of your less participation? * Rate your answer on the scale of 1 (Strongly Disagree) to 6 (Strongly Agree) *Select only one option per row*

	1	2	3	4	5	6
The task was too easy	○	○	○	○	○	○
UnRizkNow forum is not a suitable tool	○	○	○	○	○	○
The forum was launched too late	○	○	○	○	○	○
Afraid that the other groups would not contribute as much (low return on investment)	○	○	○	○	○	○
UnRizkNow is unreliable	○	○	○	○	○	○

6. Any other reasons:

7. What should we have done differently with UnRizkNow so that you could have taken advantage of it?

8. Did you ever refrain yourself sharing information on UnRizkNow even if you wanted to share? * *Select only one option*

○ Yes, ○ No

9. If you answered yes to the previous question, can you briefly explain why you decided to do that?

10. What other tools did you use for sharing information within the group? * *Check all that apply*

☐ Facebook, ☐ Google Disk, ☐ Dropbox, ☐ Sharelatex, ☐, Microsoft office 365, ☐ Skype, ☐ GitHub, ☐ Sharepoint, ☐ Other:

15.2 Questionnaire 2: A survey on information sharing practices

This section presents the list of questions used to collect data in chapters 9 and 10.

15.2.1 Information sharing

1. How frequently do you use the following medium to share your professional information with others?

- Face to Face meeting
- Online Forum
- Email
- Social media (Facebook, Twitter, LinkedIn, etc.)

2. To what extent do the following factors increase your willingness to share information with others? [Rate your answer on the scale of 1 (Not at all) to 7 (Extremely)]

- Privacy Policy (use of chatham House rule)
- Trust with information recipient (Known participants)
- Incentive for sharing (knowledge, money, fame)
- Having an online platform (forum)
- Meeting in person (Face to face setting)
- Possibility to share information anonymously

3. To what extent the following tasks would have a positive impact solving your professional problems? [Rate your answer on the scale of 1 (Not at all) to 7 (Extremely)]

- Sharing your information with others
- The response that you receive from others

4. To what extent would you consider the following factors as a barrier if you were to share your professional information with others? [Rate your answer on the scale of 1 (Not at all) to 7 (Extremely)]

- Losing competitive advantage
- Concern of receiving irrelevant information
- Different cultures, origins
- Privacy concern
- Sensitivity of the information
- Limited IT capability (lack of suitable tool, platform)

15.2.2 Community of practice

5. Have you ever participated in a knowledge sharing community (Community of Practice)?

- yes
- No

6. How did you participate in the community of practice?

- Online community of practice (a web portal, web forum)
- Offline discussion in a community (Face to face meeting, roundtable discussion)
- Both online and offline
- Other

7. What was the domain (area) of the community that you participated in?

- Information security
- Software Engineering
- IT management
- Health, environment, and safety

8. What was/were your role(s) in the community of practice?

☐ Sponsor [One who provides funds, Manage official relationships]

☐ Organizer [Ensure and articulate a valid purpose behind a CoP, Organize face-to-face gatherings when needed]

☐ Member [Share knowledge and experiences, participate in discussions and other sessions, etc.]

☐ Facilitator [Clarify communications, Keep discussions on topic, Ensure that dissenting points of view are heard and understood]

☐ Leader [Identify emerging trends and patterns in CoP activities and knowledge base]

☐ Other

9. How well the following factors scored in the community of practice that you participated in? [Rate your answer on the scale of 1 (Not at all) to 7 (Extremely)]

- Incentives or rewards for participation

- Lowering barriers among members to get involved in knowledge-sharing activities
- Keeping community focus on its purpose
- Securing trust of shared information
- Have a clear policy on information sharing outside the community

10. To what extent the following features are important to you to join an ONLINE community of practice? [Rate your answer on the scale of 1 (Not at all) to 7 (Extremely)]

- The community is always available and can be consulted when needed
- The community allows various geographically dispersed units/practitioners to work together
- Membership fee to join the community
- The way community handles privacy and confidentiality issues
- Sharing my experiences with others to help them
- Improving your knowledge, through exposure to novel problems
- Building reputation among the community members

15.2.3 Demography

This section of the survey covers a few questions on age, profession, etc.

11. Please specify your gender.

- Male
- Female
- No answer

12. What is your age group?

- Under 25 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55-64 years old
- 65 years or older

13. Who are you affiliated with?

- University
- Industry
- Public sector
- Research Institute
- Retail
- Private Organization
- Other

14. Which of the following options does describe your primary occupation?

- Chief information security officer
- Business, management, or financial (e.g., manager, accountant, banker)
- Administrative support (e.g., secretary, assistant)
- Security engineer
- Legal (e.g., lawyer, law clerk)
- Scientist (e.g., researcher, professor)
- IT professional (e.g., systems administrator, programmer)
- Decline to answer
- Other:

15. What is the size of the organization where you are working now?

- 0-5 employees
- 6-50 employees
- 51-100 employees
- more than 101 employees

15.2.4 Final

This is the final section of the survey. You may add a comment to tell us something that might be relevant to us, and not covered in this survey.

16. Any other comments?

15.3 Questionnaire 3: Information sharing practice

This section presents the list of questions used to collect data in chapter 11.

15.3.1 Demography

1. What is your age group (in years)? Choose one of the following answers

- 21-30
- 31-40
- 41-50
- 51-60
- >60

2. Please specify your gender. Choose one of the following answers

- Female
- Male
- Decline to answer

3. What is the highest level of formal education do you have? Choose one of the following answers

- Primary school
- High school graduate, diploma or the equivalent
- Bachelor's degree
- Trade/technical/vocational training
- Associate degree
- Master's degree
- Doctorate degree
- Professional degree
- Other

4. Please select the country where you are currently employed. Choose one of the following answers

- Norway
- Other

5. What best describes the type of organization you work? Choose one of the following answers

- Financial and insurance

- Mining and extraction
- Information and communication
- Agriculture, forestry and fishing
- Electricity, gas, damp, and heating supply
- Transport and storage
- Accommodation and service
- Health and social services
- Production industry
- Business service
- Culture, entertainment and leisure
- Other

6. Which of the following most closely matches your job role? Choose one of the following answers

- Chief Information Security Officer (CISO)
- Data protection officer
- Security Engineer
- Legal (advocate)
- IT professional (Systems administrator, programmer)
- Journalist
- Researcher
- Administrative (e.g. secretary, assistant)
- Accountant
- Other

7. Counting all locations where your employer operates, what is the total number of persons who work there? Choose one of the following answers

- 0-10
- 10-49
- 50-99
- 100-499
- 500-999
- 1000-4999
- 5000-
- I don’t know

15.3.2 Work activities

8. How many hours per week do you spend on information security related tasks in your job responsibilities? Choose one of the following answers

- 0-10
- 11-20
- 21-30
- 31-40
- 41-

9. Which of the following tasks do you perform daily? Check all that apply

- ☐ Develop an information security policy for the organization
- ☐ Co-ordinate the information security activities at the organizational level
- ☐ Share my expertise with my colleagues inside the organization
- ☐ Share my expertise with my colleagues outside the organization
- ☐ Perform risk and threat analysis of the information security for the organization
- ☐ Reporting to the top management team about the information status of the organization

10. What is the most frequent activity do you perform to carry out your job tasks? Choose one of the following answers

- Look for information [**N1**]
- Process information [**N2**]
- Create new information [**N3**]
- Solve problems [**N4**]
- Make decision [**N5**]
- Interact with the peers [**N6**]
- Help others to do their job [**N7**]
- Other [**N8**]

11. Which source do you mostly use to obtain the necessary information needed to carry out your tasks? Choose one of the following answers

- Personal experience [**S1**]

- Government Agency (e.g. Datatilsynet) [**S2**]
- Asking other professional experts on Communities of practice [**S3**]
- Consultancy firm [**S4**]
- Interview/meeting with your team [**S5**]
- Internal document/manual of your company [**S6**]
- Social media (e.g. LinkedIn) [**S7**]
- Other [**S8**]

12. What is the most challenging part in obtaining the information required to complete your tasks? Choose one of the following answers

- The information is available in the fragmented manner [**C1**]
- The information is outdated and cannot be applied to recent problems [**C2**]
- The information is untrustworthy as I don't know the source [**C3**]
- The information is difficult to find, time-consuming [**C4**]
- The information has a low relevance to my problem [**C5**]
- Other **[C6]**

15.3.3 Community-based knowledge sharing

13. Do you participate in a community-based knowledge sharing practice?

- Yes
- No

14. What is the domain of the community where you are mostly an active member? [answer only if you select 'yes' in Q13]

- Information security
- Other

15. Please select the statement that is valid for the community where you participate most. [answer only if you select 'yes' in Q13]

- The community has both online and offline activities
- The community has only online activities
- The community has only offline activities

16. What is the estimated number of members in the community? [answer only if you select 'yes' in Q13]

- 10-99
- 100-499
- 500-999
- >1000
- I don't know

17. Please mark the statement(s) that is(are) valid for you in terms of participating in the community-based knowledge sharing tasks. Check all that apply

☐ My knowledge is very personal to me. I don't like to share it with others [**SQ01**]

☐ Sharing my knowledge improve my reputation within the community [**SQ02**]

☐ When I share my knowledge in the community, I expect to get back knowledge whenever I need it [**SQ03**]

☐ When I share my knowledge in the community, I believe that my questions will be answered in the future [**SQ04**]

☐ Sharing my knowledge with others gives me pleasure [**SQ05**]

☐ My knowledge sharing with other members is valuable to me [**SQ06**]

☐ I do not share anything as I am concerned about the sensitivity of my information [**SQ07**]

☐ Members on the community share information relevant to my problems [**SQ08**]

☐ I share my knowledge only when the community has the option for the face-to-face communication [**SQ09**]

☐ Participating in the community decreases the time needed for my job responsibilities [**SQ10**]

☐ Participating in the community increases the effectiveness of performing job task [**SQ11**]

☐ I have the resources necessary to share knowledge in the community [**SQ12**]

☐ I participate in the community to establish new connection with the members [**SQ13**]

☐ People who are important to me expect that I should participate in the knowledge sharing task in the community [**SQ14**]

☐ By sharing knowledge within community, I find better solution for my problem [**SQ15**]

☐ I share the work reports and official documents obtained from inside the organization with other members [**SQ16**]

- ☐ I share my expertise from my education, training, experience with other members [**SQ17**]
- ☐ I trust the information that I receive from other members in the community [**SQ18**]
- ☐ I trust the information only if I know the identity of the member whom I am sharing my knowledge with [**SQ19**]
- ☐ I get the latest (up-to-date) information/answers for my question in the community [**SQ20**]
- ☐ I do not share my knowledge on a community because I may lose my competitive edge [**SQ21**]
- ☐ My organization allows me to participate on a community-based platform to share my knowledge [**SQ22**]
- ☐ My job profile allows me to participate on a community-based platform to share my knowledge [**SQ23**]
- ☐ I have everything that I need to carry out my job tasks effectively. Therefore, I do not need to participate [**SQ24**]
- ☐ I am willing to participate if the community is available as an online platform [**SQ25**]

15.3.4 Final

18. Any other comments? Please write your answer here: _____

15.4 Questionnaire 4: A survey on information security knowledge sharing on electronic platforms

This section presents the list of questions used to collect data in chapter 12.

The survey should only take 10-12 minutes. This survey is completely anonymous. The record of your survey responses does not contain any identifying information about you. You can submit your response by pressing the 'Submit' button at the end of the survey. If you feel that the response to any question can breach your privacy, you may discard your survey participation by NOT pressing the 'Submit' button at the end of the survey.

15.4.1 Demography

1. What is your age group (in years)? Choose one of the following answers

   - 21-30

- 31-40
- 41-50
- 51-60
- >60

2. Please specify your gender. Choose one of the following answers

- Female
- Male
- Decline to answer

3. What is the highest level of formal education you have?

- Primary school
- High school
- College (Bachelor's degree or similar)
- University (Master's degree or above)
- I decline to answer
- Other

4. Please select the country where you are currently employed. Choose one of the following answers

- Norway
- Other

5. Which of the following most closely matches your job role?

- CEO
- Chief Information Security Officer (CISO)
- Security consultant
- Security Engineer
- Data protection officer
- Risk advisor
- Auditor
- Legal (advocate)
- Researcher

- IT professional (Systems administrator, programmer)
- Administrative (e.g. secretary, assistant)
- Journalist
- Accountant
- Sales Manager
- I decline to answer
- Other

6. What best describes the type of organization you work?

- Financial and insurance
- Mining and quarrying
- Information and communication
- Agriculture, forestry and fishing
- Electricity, gas, damp, and heating supply
- Transport and storage
- Accommodation and food service
- Health and social services
- Construction
- Public administration and defense
- Culture, entertainment and leisure
- Other

7. Counting all locations where your employer operates, what is the total number of persons who work there?

- 0-10
- 10-49
- 50-99
- 100-499
- 500-999
- 1000-4999
- 5000-
- I don't know

8. How many hours per week do you spend on information security tasks?

- 0-10
- 11-20
- 21-30
- 31-40
- 41-

15.4.2 Information security (IS) knowledge sharing

In this section, IS knowledge refers to all intelligible ideas, information and data in whatever form in which it is expressed or obtained in the field of Information Security. IS knowledge is required by information security professionals to carry out their regular tasks. IS knowledge can be:

A method to compare different risk management methods.

Details of risk assessment phase

Details of new anti-virus installed in the organization

The reports on IS incidents

9. Which of the following communication tools do you use regularly for information security knowledge sharing?

- ☐ SMS
- ☐ Email
- ☐ Telephone
- ☐ Facebook
- ☐ Twitter
- ☐ Electronic communities of practice
- ☐ Formal meetings
- ☐ Training/workshop
- ☐ Video/phone conference
- ☐ LinkedIn
- ☐ Blog

10. To what extent do you agree or disagree with the following statements: (Rate your answer on the scale of 1- Strongly disagree, 2- Disagree, 3- Undecided, 4- Agree, 5- Strongly Agree)

- I share my IS knowledge on electronic platform to solve the problems of other members

- I seek IS knowledge on electronic platform to solve my problems
- I apply IS knowledge that I receive on electronic platform to solve my problems
- I share my IS knowledge with my colleagues on electronic platform to increase their awareness
- I inform other staff about new methods and software related to IS on electronic platform
- I share the reports on IS incidents with my colleagues inside the organization on electronic platform
- I share the reports on IS incidents with my colleagues outside the organization on electronic platform

11. I share my information security knowledge on electronic platforms because (Rate your answer on the scale of 1- Strongly disagree, 2- Disagree, 3- Undecided, 4- Agree, 5- Strongly Agree)

- I believe that it is important to share IS knowledge with other professionals
- I enjoy helping other members by sharing my IS knowledge
- It improves my reputation in the IS community
- It helps me building relationships and network with other IS professionals
- It provides me gaining expert status in the IS community
- It enables my superior to believe that I am competent in the area of IS
- It helps me achieve better results (quality, productivity) in projects and programs under the IS domain
- It helps in capturing and storing IS knowledge so that it could be easily accessed and applied whenever I need it
- I receive monetary benefits (reward, promotion, salary hike)

12. To what extent do you agree with the following statements related to your information security knowledge sharing preferences on electronic platforms? (Rate your answer on the scale of 1- Strongly disagree, 2- Disagree, 3- Undecided, 4- Agree, 5- Strongly Agree)

- I share my IS knowledge on electronic platforms only anonymously as I am concerned about my privacy
- I share my knowledge on electronic platforms only with the members whom I know personally

- I trust the content on electronic platforms only if it is validated by other IS professional (by means of rating, voting)
- I trust the IS knowledge on electronic platform only if I can see the true identity of the member (who shared the information)

13. To what extent do you agree or disagree with the following statements based on your experience of participating in IS knowledge sharing activities on electronic platforms? (Rate your answer on the scale of 1- Strongly disagree, 2- Disagree, 3- Undecided, 4- Agree, 5- Strongly Agree)

- I received knowledge from others whenever I needed it on electronic platform
- I received latest (up-to-date) IS knowledge from other professionals on electronic platform
- It was easy for me to trust the credibility of IS knowledge shared on electronic platform
- The IS knowledge was available in a structured and collected manner on electronic platform
- It was easy for me to find a specific IS information on electronic platform
- The IS knowledge on electronic platform was relevant to my domain and concern

14. To what extent do you agree or disagree with the following statements: (Rate your answer on the scale of 1- Strongly disagree, 2- Disagree, 3- Undecided, 4- Agree, 5- Strongly Agree)

- My current job allows me to share my IS knowledge with other IS professionals on electronic platform
- I have enough time to share my IS knowledge on electronic platform
- I have enough training and skills to use electronic platforms to share my IS knowledge
- My organization allows me to share my IS knowledge outside the organization
- I share my IS knowledge on electronic platform only after careful consideration of the consequence
- My IS skills have been improved by sharing my IS knowledge on electronic platform