TUCS

Ali Farooq

In Quest of Information Security in Higher Education Institutions

Security Awareness, Concerns and Behaviour of Students

Turku Centre for Computer Science

TUCS Dissertations
No 245, November 2019

In Quest of Information Security in Higher Education Institutions

Security Awareness, Concerns, and Behaviours of Students

Ali Farooq

To be presented, with the permission of the Faculty of Science and
Engineering, for public
criticism in the Auditorium Natura X on November 22, 2019 at 12:00.

University of Turku
Department of Future Technologies
Vesilinmantie 5, 20500, Turku, Finland

2019

Supervised by

Professor Jouni Isoaho
Department of Future Technologies
University of Turku
Finland

Associate Professor Seppo Virtanen
Department of Future Technologies
University of Turku
Finland

Reviewed by

Professor Karen Renaud
Department of Cyber Security
Abertay University
Dundee, United Kingdom

Professor Martti Lehto
Faculty of Information Technology
University of Jyväskylä
Jyväskylä, Finland

Opponent

Professor Sascha Fahl
Head, Information Security Chair
Department of Computer Science
Leibniz University
Hanover, Germany

ISBN 978-952-12-3879-6
ISSN 1239-1883

To my paternal grandfather who raised a thirst of knowledge in me

To my maternal grandfather who introduced me to the power of observation

Abstract

Humans, often suggested as the weakest link in information security, require security education, training and awareness (SETA) programs to strengthen themselves against information security threats. These SETA programs improve security awareness (also called information security awareness or ISA) which makes users conscious about the information security threats and risks and motivates them to learn knowledge and measures to safeguard their information security.

Studies have shown that most of the SETA programs do not achieve their desired objectives and been proven ineffective. This ineffectiveness is probably because: 1) current SETA programs are designed as a one-fits-all solution and are not tailored as per users' needs, 2) users are not included in the design phase of the SETA programs and 3) the SETA programs lack theory-grounded approaches. Nonetheless, the relationship between ISA and security behaviour also needs explanation. This thesis sets out to address the issues mentioned above.

In this thesis, four separate studies grounded in both quantitative and qualitative methods are conducted. Cross-sectional data from students of a single case was collected using online surveys, with one exception in which data was collected as part of a class assignment. The results showed that, in general, students believed they know more than they actually did. The impacts of gender, previous training, and educational discipline were evident on security knowledge, behaviour, perceived awareness and actual awareness.

Students have a wide range of security concerns, related to their personal, social, technological, non-technological and institutional dimensions of everyday life, and not just technological and non-technological aspects as shown in the existing literature. Further, students differ significantly from security experts in terms of their security practices. However, aware students (having training in information security) were more similar in security practices to security experts than the unaware students (having no formal or informal information security training). Lastly, it was found that the relationship between ISA and security behaviour can be explained using Information-Motivation-Behavioural Skills (IMB) model. The research presented in this thesis has implications for faculty members who teach students and the security professionals responsible for information security of higher education institutions.

Abstract in Finnish

Ihminen mielletään usein tietoturvan heikoimmaksi lenkiksi. Jotta tietoturvauhkilta osattaisiin suojautua, tarvitaan erillistä tietoturvakoulutusta, -harjoitusta sekä -tietoisuutta. Erilaiset tietoturvakoulutukset lisäävät henkilön tietoisuutta erilaisista tietoturvauhkista ja -riskeistä sekä motivoivat oppimaan tapoja ja toimenpiteitä, jotka parantavat henkilökohtaista tietoturvaa.

Tutkimuksissa on kuitenkin ilmennyt, että useimmat tietoturvakoulutukset eivät saavuta toivottuja tavoitteita, ja ne ovatkin osoittautuneet tehottomiksi. Tehottomuus johtuu todennäköisesti siitä, että (1) koulutuksia ei ole räätälöity käyttäjien tarpeiden mukaisiksi vaan yleisluontoisiksi, (2) käyttäjiä ei ole otettu mukaan koulutusten suunnitteluun, ja (3) koulutuksilta puuttuvat teoriapohjaiset lähestymistavat. Tässä väitöskirjassa tutkitaan yllä mainittuja epäkohtia ja selvitetään ihmisen tietoturvakäyttäytymisen ja -tietoisuuden suhdetta.

Väitöskirjassa esitetyt tulokset saavutettiin tekemällä neljä erillistä tutkimusta kvantitatiivisin (määrällisin) ja kvalitatiivisin (laadullisin) menetelmin. Tietoa kerättiin tutkimusten kohteina olleilta opiskelijoilta verkkokyselyillä, paitsi yhdessä tapauksessa, jossa kysely toteutettiin osana kurssitehtävää. Tulokset osoittavat, että yleisesti opiskelijat mielsivät tietävänsä enemmän kuin todellisuudessa tiesivät. Sukupuolella, aiemmalla koulutuksella ja tieteenalalla oli selkeä vaikutus vastaajien tietoturvakäytökseen - sekä miellettyyn että varsinaiseen tietoisuuteen.

Opiskelijoilla on monenlaisia tietoturvaan liittyviä huolenaiheita, jotka liittyvät persoonallisiin, sosiaalisiin, teknologisiin, ei-teknologisiin sekä arkisiin ulottuvuuksiin. Tämä poikkeaa nykyisen kirjallisuuden näkemyksestä, joka käsittää vain teknologisen ja ei-teknologisen ulottuvuuden. Opiskelijat eroavat merkittävästi tietoturva-asiantuntijoista tietoturvakäytäntöjensä suhteen. Tietoturvakoulutusta saaneet, tietoisemmat opiskelijat olivat käyttäytymiseltään lähempänä tietoturva-asiantuntijoita kuin vähemmän tietoiset ja vähemmän koulutusta aiheesta saaneet opiskelijat. Tutkimuksessa kävi ilmi myös, että tietoturvatietoisuuden ja -käyttäytymisen välistä suhdetta voidaan selittää käyttäen IMB-mallia (Information-Motivation-Behavioural Skills model). Tässä väitöskirjassa esitetty tutkimus ja sen tulokset ovat korkeakoulujen opetushenkilöstön ja tietoturvasta vastaavien ammattilaisten suoraan hyödynnettävissä.

Publications

The content of this thesis (key aspects, ideas and figures) has been previously appeared as parts in the following publications, in chronological order:

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015, August). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In Trustcom / BigDataSE / ISPA, 2015 IEEE (Vol. 1, pp. 352-359). IEEE.

Farooq, A., Isoaho, J, Virtanen, S. & Isoaho, J.(2015). Observations on Genderwise Differences among University Students in Information Security Awareness. *International Journal of Information Security and Privacy, 9(2), 59-73, April-June 2015*

Farooq, A., Kakakhel, S. R. U., Virtanen, S., & Isoaho, J. (2015, December). A taxonomy of perceived information security and privacy threats among IT security students. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 280-286). IEEE.

Farooq, A., Alifov, S., Virtanen, S., & Isoaho, J. (2018, July). Towards comprehensive information security awareness: a systematic classification of concerns among university students. In *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32* (pp. 1-6).

Farooq, A., Jeske, D., & Isoaho, J. (2019, June). Predicting Students' Security Behavior Using Information-Motivation-Behavioral Skills Model. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 238-252). Springer, Cham.

In addition to above, following pieces of research, not directly related to the thesis but influences the thesis, have been produced by the author in collaboration with local and international researchers:

Farooq, A., & Kakakhel, S. R. U. (2013, December). Information security awareness: Comparing perceptions and training preferences. In 2013 2nd National Conference on Information Assurance (NCIA) (pp. 53-57). IEEE.

Farooq, A., Balakrishnan, L., Phadung, M., Virtanen, S., Isoaho, J., Poudel, D. P., & Isoaho, J. (2016, August). Dimensions of Internet Use and Threat Sensitivity: An Exploratory Study among Students of Higher Education. In Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), 2016 IEEE Intl Conference on (pp. 534-541). IEEE.

Khadam, N., **Farooq, A.** & Alwadei, S., Individual Differences and E-Learning Acceptance among Saudi Students. 21st Saudi Computer Society National Computer Conference (NCC), 2018. IEEE

Faroq, A., Ndiege, J. R., Isoaho, J. (2019, September). Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior. In *IEEE Africon'19.* 2019. IEEE. [Accepted]

Acknowledgements

First, I would like to thank Allah Almighty, the Most Gracious, the Most Merciful, for giving me the ability to complete my PhD. Then, I want to thank everyone who has contributed to the accomplishment of this thesis, starting with my supervisors Prof Jouni Isoaho and Associate Prof Seppo Virtanen. This journey was never possible without the support provided by both. Both supported me throughout the PhD and gave me freedom which not only allowed me to develop my research skills but also, enabled me to establish several collaborations beyond this thesis.

I cannot express my gratitude in words for my parents, who encouraged me throughout my life, and always supported me to go for what I want. "I would have been nothing without you, *Ammi Abu*". I am also grateful to my wife and my kids who supported me, who forgo their time so that I could concentrate on my PhD. It has been a great sacrifice on their parts.

I also want to mention few others who one way or another has a supporting role in the PhD journey, and thank them. The journey into the field of IT was not possible without the support of my uncle Zaki Babar, who arranged for my first ever computer in 2000. I thank Mr Awais Ahmad, Director General, Higher Education Commission (HEC), Pakistan for encouraging me to pursue my ambitions and for a PhD. He was my supervisor and mentor when I was working as Assistant Director in HEC.

I also want to thank my friend and colleague, Syed Rameez Ullah Kakakhel, for been there throughout the PhD journey, and even before that. He listened to my frustrations, cheered me up, supported me and gave me insights on my work from time to time.

Table of Content

List of Figures

List of Tables

Acronyms

AIDS	Acquired Immune Deficiency Syndrome
AISA	Actual Information Security Awareness
ANOVA	Analysis of Variances
AVE	Average Variance Explained
CBAM	Concerns-based Adoption Model
CR	Composite Reliability
CVC	Customer Verification Code
GDT	Generation Deterrence Theory
HEI	Higher Education Institutions
HU	Home Users
IMB Model	Information-Motivation-Behavioural Skills Model
IT	Information Technology
ICT	Information & Communication Technologies
ISA	Information Security Awareness
ISP	Information Security Policies
NHU	Non-home Users
OS	Operating System
PISA	Perceived Information Security Awareness
PCA	Principal Component Analysis
PMT	Protection Motivation Theory
SETA	Security Education, Training and Awareness
SEM	Structural Equation Modeling
SPSS	Statistical Package for Social Sciences
TPB	Theory of Planned Behaviour

TAM	Technology Acceptance Model
TRA	Theory of Reasoned Action
TVE	Total Variance Explained

Chapter 1
Introduction

In today’s world, the Internet has become the backbone of our societies and businesses. Both individuals and organisations use this technology to gather a variety of technical and social benefits. The organisation has implemented information systems backed by the Internet to ease out their operations and maximise their output, whereas, the individual user makes use of the Internet for several purposes ranging from information gathering to entertainment, and from shopping to socialising. The around-the-clock access of the internet at one end provides numerous opportunities for both individuals and organisations, at the other, exposes the users to many challenges including information security risks [3], [4]. Organisations employ a variety of technical solutions such as firewalls, backups, and anti-malware software, to improve their information security. However, these are proven insufficient due to failures caused by the users - making users the weakest link in the information security [5]–[7]. A recent study showed that 27% of security breaches in organisations were due to process failure, whereas 25% was due to the negligent behaviour of the employee [8]. However, it is not clear from the study if the incidents were overlapping or otherwise. To strengthen this weakest link, Organisations adopt non-technical measures such as policies, and security education, training and awareness (SETA) programs to improve human ability to deal with the information security threats[9]–[12]. These SETA programs improve security awareness (also called information security awareness or ISA) which make users conscious about the information security threats, risks, and motivates them to learn knowledge and measures to safeguard their information security [13]–[15]. Users' security behaviours are affected by their perception of information security threats [16], whereas, ISA improve their understanding of possible threats and the countermeasures that can be used to safeguard their information security. In short, ISA helps users in decision making in the event of security threat. Due to these reasons, ISA has been regarded as the most significant indicator of the overall information security situation in an organisation [10], [17], [18] as well as one of the essential prerequisites of users' security behaviour [10], [15], [19].

Like other organisations, educational institutions, notably higher education institutions (HEIs), are heavily dependent on information technology (IT) for their operations and decision support activities ([20], [21]), as well as for storing and maintenance of a significant amount of private information of students, faculty members and staff [22]. The availability of a vast amount of computing power, personal information of students and employees, and information assets related to cutting edge research make HEIs attractive to both cybercriminals and insider threats. A recent surge of information security incidents [23]–[25] is an indication of what HEIs should expect in the coming days. However, HEIs are not ready to deal with information security challenges. It has been found that HEIs do not have adequate information security mechanisms [26], [27]. The security policies in HEIs are highly techno-centric [28] and employees do not comply with them either [29]. In addition to employees, HEIs also has a large population of students who are most of the time connected to the Internet for several reasons ranging from educational to entertainment. It has been found that students are more prone to cybercrimes than employees [30]. They have been found behind data breaches incidents as well [31]. Thus, information security in HEIs is not possible without taking both populations (employees and students) into consideration.

1.1 Problem Statement

While ISA has been found as one of the significant contributors to information security of an organisation-behaviour of the users -, studies have shown that most of the

SETA programs do not achieve their desired objectives and proven ineffective [32], [33]. This is a serious problem when a proposed remedy for an issue is not giving the desired results. There are following reasons for the said ineffectiveness:

1. Awareness programs (also called SETA programs) lack the theory-grounded approaches
2. The user-centred approach is lacking; where users are not involved in the design phase of the SETA programs
3. SETA programs are usually designed as a one-fit-all solution and are not tailored as per users' needs

1. Lack of theoretical backing

Existing SETA programs lack theory-grounded approaches. To understand the relationship between ISA and security behaviour, researchers have used theories such as Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), and Protection Motivation Theory (PMT) [34]–[36]. These theories-based studies help us understand the relationship between ISA and security behaviour. Despite these studies and the evidence that existing SETA programs are ineffective, there is still room to explore and examine the relationship between ISA and security behaviour using different theory-based approaches. One thing which is common in the existing theory-based studies is that ISA has never been a constituent construct of the theory. It has always been studied as an external factor to the theory or model. For example, TRA explains the relationship of attitude and subjective norms with behavioural intention; TPB builds upon TRA and adds a construct of perceived behavioural control (often referred as self-efficacy), and PMT describes how threat appraisal and coping appraisal affect the motivation of the users to take security measures. In all the studies where the relationship of ISA with security behaviour has been studied, ISA has been used as an antecedent for the models mentioned above rather than the constituent construct. (For detail consult review study [34]). Thus, there is a need for a behavioural model where ISA is a component of the model to have a better understanding of ISA-security behaviour relationship so that both security awareness and behaviour of the users can be improved.

2. Users' involvement in the design of ISA programs

Users are not involved in the design phase of such programs. The security experts identify the areas where users' security awareness needs to be improved. Later, ISA of the users is assessed using the identified focus areas. For example, Parsons, McCormac, Butavicius and Pattinson proposed a tool to determine ISA of employees for which focus areas were identified by interviewing the security managers [37], [38]. There is hardly any evidence in the literature that users were involved in the design phase of SETA programs (a review of related research is given in Chapter 4).

3. Users' awareness needs assessment

One type of SETA program is used across the board in the organisation, without considering users' need. As mentioned earlier, threat perceptions play an important role in users' decision making. If a user does not consider an action risky, s/he will not be interested in awareness programs focused on improving that action. There is a need to identify the segment of users who need awareness training [6].

1.2 Purpose and Objectives

As mentioned in section 1.1, current studies lack tailored security awareness programs; there is a scarcity of user-centred approaches; theory-based approaches are needed to understand and improve security behaviours. The ultimate objective, in any case, is to enhance security behaviour. Although ISA has been proven to play a significant role in the improvement of security behaviour, the research on how ISA affect security behaviours is on-going and needs further investigation.

This thesis addresses the gaps mentioned in previous sections in the context of higher educational institutions by focusing on students. However, the primary purpose of this thesis is to explain the relationship of security awareness and security behaviour of students using a behavioural model that has not been used in the context of information security before. Following is the main question of the thesis:

RQ: How does information security awareness affect the security behaviour of the students?

To find the answer to the above question as well as to address the gaps stated in the previous section, following objectives are set for this thesis:

O1: To describe the relationship of information security awareness (ISA) with different individual factors of students

To conduct awareness assessment among the students, to identify, if any, student groups having a differing level of ISA, and to compare them? This objective will help in identifying the student group(s) having a different level of security awareness.

O2: To identify perceived information security threat (concerns) of the students

To understand the security concerns of the students, and to identify the areas where students perceived to have information security risks. This objective will identify perceived security threats of the students, as well as the areas which should be kept in mind for designing SETA programs.

O3: To describe differences in security behaviours of students and security expert

To examine the security behaviour of the students and to compare them with that of the security experts, to identify the differences, if any. The comparison will help us understand the role of ISA, that is if students with high awareness level perform better than lower awareness level.

O4: To explain the relationship between security awareness and security behaviour of the students

To study the relationship of ISA with students’ security behaviour using a new model, called IMB model where ISA is operationalized in the form of knowledge of threats and security measures.

1.3 Research Design and Methodology

For the studies in this thesis, a single case study was conducted. In this methodology, data is gathered from primary sources as well as secondary sources. The primary source was the data collected from the students, whereas, a literature review was used as a secondary source of data.

1.3.1 Research Approach

Scientific inquiry can take two forms: inductive and deductive [39]. The research contribution of the study is mostly dependent upon the selection and application of one of these two approaches.

The inductive approach is usually called a bottom-up approach where the research process is not guided by theory but based upon what data tells [40] — a typical example is Grounded theory. The observations from the collected data are then used to construct generalisations, understand relationships and even suggest theories. However, it cannot be said that the inductive approach does not take note of pre-existing theories or ideas when approaching a problem. The purpose of the inductive approach is to establish patterns and meanings without falsifying a theory [39].

On the other hand, the deductive approach aims at testing (confirming, refuting or modifying) a hypothesis, explaining the relationship between two or more concepts. The deductive inquiry, on the other end, is based upon an existing theory. This testing takes place in a series of steps (more detail in Chapter 6). Though inductive and deductive approaches are different, however, these are not mutually exclusive. Researchers can also combine both inductive and deductive methods to address a problem [39]. There is a separate debate if the research can be strictly inductive. Moreover, it has been proposed that both inductive and deductive inquiries are connected [41]. Sometimes the difference can only be seen in the initial framework; whether or not it is loosely or strictly grounded in the previous research [42].

In this thesis, I have used both inductive and deductive approaches. For objectives $\boldsymbol{O_1}$ to $\boldsymbol{O_3}$ an inductive approach has been used, where data is collected to examine patterns, whereas, a deductive approach has been used to achieve objective $\boldsymbol{O_4}$.

1.3.2 Research Philosophy

"Epistemology provides a philosophical background for deciding what kinds of knowledge and legitimate and adequate" [39]. Broadly there are three epistemological stances: Objectivism, Constructivism and Subjectivism [39], [43].

Objectivists believe that reality exists out there, independent of consciousness. So, knowledge is out there, and we need to discover it. Constructivists believe there is no objective truth out there. The meaning is what is constructed by the subject's interaction and engagement with the world. So, the truth or knowledge is constructed rather than discovered. The subjectivists believe that meaning is not an outcome of the interplay of subject and object, but what subject imposes on the object. Subjects create meanings through their beliefs, dreams or from within unconsciousness and objects do not have any role to play in it. The theoretical perspectives associated with objectivism, constructivism and subjectivism are positivism, interpretivism and postmodernism respectively.

Matching with the approaches - deductive and inductive - the studies presented in this thesis are associated with both positivism and interpretivism [39, 43]. Positivism supports the idea of ISA and security behaviour, where ISA is studied as an object (***O_1***), security behaviour is studied as an object and comparison are made between students and security experts (***O3***). Interpretivism supports the idea that students have different perceptions about security threats (concerns) and their security awareness, and resultantly behave differently. ***O_2*** aims at identifying and exploring the security concerns of the students. The identifying part pertains to positivism whereas the exploratory part takes the subjective interpretation of the respondents. The final objective (***O_4***), which also relates to the main research question of the thesis falls into the interpretivism paradigm.

1.3.3 Research Design

To ensure that the thesis provides reliable results, the right choice of research methodology is essential. The research design acts as a tool for planning of methods used for collecting relevant data and analysis, which are in line with the objectives of the research. According to Creswell [44], there is a need to identify the philosophical standing of the research as it directs the mode of inquiry. The philosophical standing, also termed as a research paradigm, helps in identifying both the problem under investigation and the solution to the problem [45]. In social science research, identifying the correct research paradigm is the first step in the research. However, this approach is hardly evident in users' focused research in information security even though users' studies in information security are highly dependent on theories from social sciences and psychology. The closest evidence of the use of research design is found in the information system. Cronje [1], proposed a four-quadrant model (shown in Figure 1.1) outlining the research design in the information system. This model is adapted from the four paradigms suggested by [2]. Traditionally, the knowledge cycle moves in the following way:

Describe→Explore→Explain→Develop

Here *describe* and *develop* consider knowledge as an objective whereas, whereas, *explore* and *explain* consider subjectivism. However, the traditional sequence of knowledge does not limit researchers' abilities to research in different quadrants.

To meet the stated objectives stated in section 1.2, the thesis uses a multi-faceted approach of combining exploratory, descriptive and explanatory insights. The placement of the objectives in research design can be seen in Figure 1.1. The research also involved the development of a cybersecurity course for students of different educational backgrounds, which relates to *develop* phase of knowledge cycle. However, in this thesis development and assessment of the course is not included.

1.3.4 Research Methods

Considering the breadth of the thesis, the objectives of the thesis could not be achieved through a single wave of data collection. Therefore, a series of studies, each addressing one objective was carried out over time, except for $\boldsymbol{O_3}$ where two studies were conducted to achieve the goal. The thesis is grounded in quantitative methods, except for $\boldsymbol{O_2}$ and $\boldsymbol{O_3}$ where the mixed-method and multi-method approach has been used respectively.

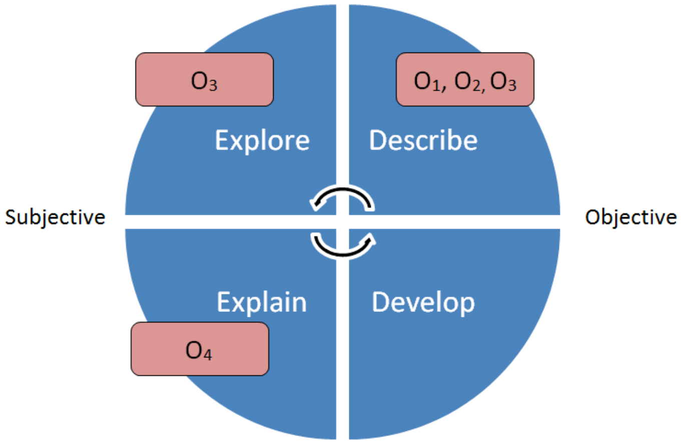


Figure 1.1: The research paradigm and design cycle (adapted from[1], [2])

The multi-method approach utilizes quantitative and qualitative methods to form independent parts of the study (Qual+Quan). Both methods (Qual and Quan) are used to answer different part of the research question. Whereas, in the mixed-method approach, both quantitative and qualitative methods are interconnected in a fashion that cannot be separated (For example, Qual->Quan or Quan->Qual). Both methods (Qual and Quan) used to answer the research question together.

A literature review was conducted for each objective, focusing on ISA and security behaviour. Empirical data for the objectives were collected through cross-sectional surveys. For each study, data was collected using online surveys, except for ***O₂*** where qualitative data was collected as part of the course assignment. The data for ***O₁,*** ***O₂*** and ***O₃*** were analysed using statistical techniques ranging from simple descriptive analysis to factor analysis in SPSS v24.0, and v25.0 whereas, data for ***O₄*** was analysed using structural equation modelling (SEM) in SmartPLS v3.0. Further detail on research methods is given separately in respective chapters. The research methodology used in this thesis is outlined in Table 1.1.

As mentioned earlier, a single case study approach was used for the studies in this thesis. The organisation is located in Turku, a southwestern city of Finland. The target population of the studies were undergraduate and post-graduate level students. The target university had a population of about 17000 students enrolled in seven different faculties at the start of this research (2014-15).

Objective	**Method**	**Unit of Analysis**	**Unit of Observation**
O_1	Quantitative	ISA	Students
O_2	Mixed (Qual->Quan)	Concerns	Students
O_3	Multi (Qual+Quan)	Security Behaviour	Students
O_4	Quantitative	ISA & Behaviour	Students

Table 1.1: The research methodology used in the thesis

1.5 Delimitation

The studies presented in this thesis are focused on information security of higher education institutions and have some limitations. For example, only students are taken as the audience of the studies, leaving out employees (faculty members and other staff). Furthermore, the research was conducted in the Department of Future Technologies, previously known as the Department of Information Technology and, therefore, most of the respondents were from IT, computer science or computer engineering backgrounds. Although data were collected from students of non-IT disciplines as well, they may not represent the whole student population of students from other disciplines. Moreover, many students work in addition to studying. This study looks at the information security issue in the context of educational institutions only, and therefore the participants were asked to consider themselves as students while answering the surveys.

The studies presented in this thesis are based on online (web-based) surveys. Such surveys are subject to self-selection bias [46] and may attract only those respondents who were comfortable with web-based surveys and have interest in the topic. Moreover, surveys provide a limited picture of what participants remember or what they are ready to share [47]. For the sake of this thesis, it is assumed that respondents of the studies have accurately reported their information security awareness, concerns and behaviours.

Considering that information security is a broad topic (as we will see in chapter 4) and many areas should be taken into consideration while assessing awareness and behaviours. Including all the areas in awareness assessment and security behaviour could lead to long surveys. The lengthy surveys not only adversely affect the response rate but also cause respondents to response without due attention. Therefore, I have been selective in picking area(s) in awareness and behaviour studies (Chapter 3, 5 and 6). The selection was made considering the most common concerns of students and security advice suggested by the security experts.

1.6 Thesis Structure

The remainder of this thesis is divided into seven chapters.

Chapter 2 provides a review of relevant literature where two main themes are discussed: (1) On the understanding of information security awareness, and (2) theories used in studying security behaviours. The purpose of this chapter is to introduce readers to the concept of information security awareness, how it is defined and assessed. Further, the popular theories used for studying information security behaviours are described.

Chapter 3 describes an assessment study where information security awareness of students of different backgrounds is assessed, and a comparison of awareness is made among students divided based on their demographics, individual and cultural factors. This chapter covers objective 1.

Chapter 4 presents a two-phase study where a mixed-method (Qual->Quan) design is used for identifying and describing information security concerns of the students. Objective 2 of the thesis is covered in this chapter

Chapter 5 describes a comparative study where a multi-method (Qual+Quan) design is used to identify security measures taken by the students, along with data on their security practices. Next, a comparison of security practices was made with that of security experts to identify the gaps. The chapter starts with an introduction, followed by related work. The methodology of the study is explained next. Results describe the comparison of practices related to system security, email security, web security and access control. The conclusion comes at the end. This chapter is related to Objective 3.

Chapter 6 presents a study where the relationship of security awareness and security behaviour is empirically validated. Like previous chapters, this chapter is also organised into an introduction, related work, methodology, results and conclusion. Objective 3 of the thesis is covered in this chapter.

Chapter 7 of the thesis provides a synthesis of findings and conclusion for the thesis.

Chapter 2
Literature Review

This chapter presents a review of literature related to this thesis. A holistic view of relevant research, starting from the concepts to the related work is given in this chapter. The chapter begins with introduction to the concepts of information security, information security awareness, what are the factors that precede ISA and what are the outcomes. Further, a theory based on an understanding of the role of concerns is provided. Next, most essential theories used so far for studying information security behaviours are discussed. Lastly, a new model (Information-Motivation-Behavioural Skills Model) is described.

2.1 Understanding Information Security Awareness

Security education, training and awareness (SETA) programs have been suggested as a non-technical tool for information security [10], [48]. In this regard, information security awareness (ISA) is considered as an essential variable that influences the security behaviour of the users. The current literature on ISA can be divided into five categories [49]:

1) Defining and conceptualisation of ISA,
2) Studying the relationship between ISA and security behaviour,
3) antecedents of ISA,
4) SETA programs, and
5) the assessment of ISA.

However, before describing existing research on ISA, lets first clarify the terms information security and cybersecurity, that are most often used interchangeably.

2.1.1 Information Security vs Cybersecurity

The five basic needs drive human behaviours: psychological, safety, social, esteem and self-actualisation [50]. These needs exist in hierarchal form, where once the first need is fulfilled, the person tries to meet the next need. When Maslow presented his famous model [50], the safety was related to real-life safety. However, since the advent of the Internet, the need for safety also exists in the online world. Since the Internet is a big system where human is presented through the digital footprint (information) s/he shares, the concept of information security is of importance.

Traditionally online safety is related to information security which has been defined differently in the literature. According to International Standard Organization standard ISO/IEC 27001, information security in an organisational context is defined as "the protection of the information from a wide range of threats to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities". Cherdantseva & Hilton [51] defined information security as "a multidisciplinary area of study and professional activity which is concerned with the development and implement of security countermeasures of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and distributed, free from threats." In addition to term information security, the online safety has been covered using terms such as computer security, IT security, ICT security, data security and the most recently the term cybersecurity (or it's variant cyber-security) is somewhat popularly used [52]. Researchers often use information security and cybersecurity interchangeably, however, there is a difference. For example, von Solms & van Niekerk (2013) discussed both information security and cybersecurity and provided a theoretical understanding as to what is the difference between the two concepts. According to them, the purpose of information security is to security assets (information assets) from a variety of threats that exploit vulnerabilities in the system (ICT). Whereas, cybersecurity ensure the safety of a broader set of assets (including humans and their interest) from a variety of threats that may exploit vulnerabilities that may exist due to the system (ICT) or the information itself. The relationship between the concepts above is shown in **Figure 2.1**.

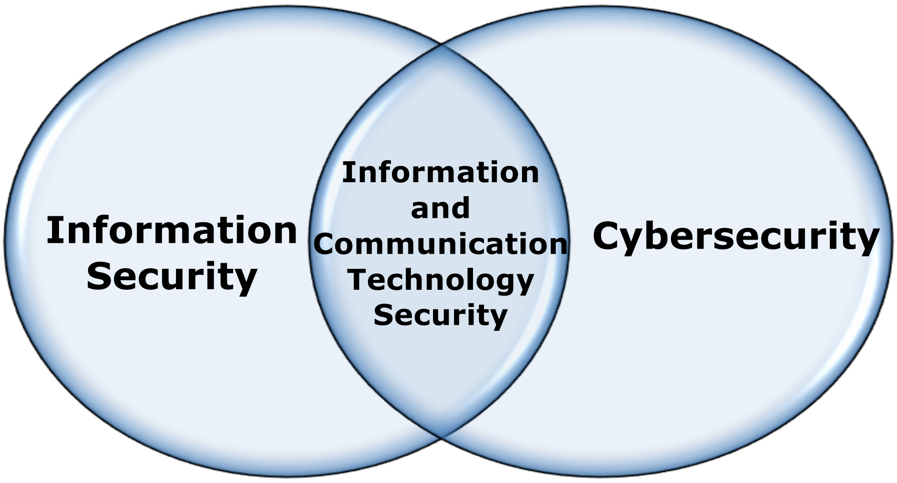


Figure 2.1: The relationship between information security and cybersecurity (adapted from [53])

2.1.2 Defining Information Security Awareness

There is no generally agreed-upon definition of information security awareness (ISA), and perhaps this is mainly due to informal and socially constructed nature of the concept [54]. The reviews of the literature on ISA [34], [49] suggest that ISA is not just a representation of the cognitive state of mind (that is being aware of information security problems). Some researchers do not differentiate between ISA and the behaviour, while others consider it a procedure to achieve the cognitive state of mind.

Firstly, ISA is considered as a cognitive state of mind has defined and used ISA differently. For example, some regards it as knowledge of security measures that users should have for their individual as well as organisational security [55]–[58]. While others believe ISA is about improving the consciousness of users by highlighting information security issues and the strategies/measures to deal with such problems [19], [59], [60]. Another group of researchers, consider ISA makes users conscious about the significance and importance of information security for individuals as well as an organisation [15], [18], [61].

Secondly, there are several definitions of ISA found in ISA literature where ISA does not depict a state of mind but connects ISA with security behaviour so tightly that it is hard to differentiate between ISA and behaviour. For example, ISA is considered as acting or responding to organisations' security policies [10], [62]–[65] to "bring committed to the security mission" [15], [26], [66]. And sometimes, it is regarded as one type of security behaviour [60].

Thirdly, ISA is considered a process by some of the researchers. The researchers who consider ISA as a process regards ISA as a process of awareness-raising activities and their management [54]. Lim et al., (2010) defined ISA as a method "to teach employees to be conscious about information security policies and procedures", whereas, Peltier [67] stated ISA as a tool "to stimulate, motivate, and remind the audience what is expected of them." According to Tsohou et al. [54], it is "an inter-functional process (check, act, plan, do) that crosses different divisional units or departments of organisations."

In this thesis, ISA is used as an awareness of security measures and knowledge of security threats. Moreover, it has been regarded as a cognitive state of mind (Chapter 3, 5) and as a process (in Chapter 4).

2.1.3 Information Security Awareness Assessment

Considering the importance of information security awareness (ISA), researchers have conducted quite a few studies using different methods in different contexts. A review of the literature suggests that researchers have used as many as ten distinctive assessment methodologies to assess ISA, which is: value-focused, survey-based questionnaire, vocabulary test, observation, interviews, game tools, E-learning, focus groups, document reviews and responses to email [68]. The target audience is the end-users in organisations, whereas, few studies were found to be focused on users from educational institutions, novice internet users and social media users. The researchers have assessed general security awareness, level of security awareness, knowledge, attitude, behaviour, information assurance, information security management awareness and reporting awareness in such studies (For detail consult [68]).

Some of the studies where ISA of the users has been assessed are tabulated in **Table 2.1**. The detail includes the purpose, scope of the study, assessment methodology, and target audience where users' information security awareness has been assessed.

The examination of the literature on ISA reveals that researchers have created tools for ISA assessment. For example, Kruger & Kearney [69] proposed a value-based assessment method, where knowledge, attitude and behaviour or employees was assessed in six focus areas based on vocabulary testing approach [70]. Building on work of Kruger & Kearney [69], Parsons, Cormac, Butavicius, Pattinson and Jerram [38] proposed a Human Aspects of Information Security Questionnaire (HAIS-Q) to determine information security awareness of organisational employees. This questionnaire assesses users' awareness in six focus areas with the help of 63 statements measuring knowledge, attitude and behaviour on 5-point Likert scale measurements. The areas are password management, email use, internet use, social networking site use, incident reporting, mobile computing and information handling.

Ref	Purpose of the study	Scope	Method	Target User
[71]	To identify internet users′ awareness of cyber threats and their understanding of the methods for protecting and safeguarding data and systems over the internet	Awareness level	Survey-based questionnaire	Home users
[26]	To explore the level of information security awareness	Security in general, the Awareness level	Observation, Document review, Interview, Survey-based questionnaire	Employees
[72]	To determine the role of learning in the workplace and home on information practice in general	Awareness level	Survey-based questionnaire	Employees & Home users
[10]	To assess the role of information security awareness and its relationship to human behavioural elements	Information assurance	Survey-based questionnaire	Employees
[73]	To identify the status of information security awareness for developing effective security awareness training in the future	Awareness level, Attitude	Survey-based questionnaire	Students
[74]	To assess the characteristics of security practices, level of awareness, countermeasure strategies as well as the compliance level of student	Security in general	Survey-based questionnaire	Students

Table 2.1: Previous literature on information security awareness, depicting the purpose, scope, method and target user (Adapted from [68])

Ref	Purpose of the study	Scope	Method	Target User
[75]	To determine the level of security culture among employees	Awareness level, Reporting	Survey-based questionnaire	Employees
[76]	To determine a methodology that can be adapted to evaluate security awareness programs	Knowledge, Attitude	Survey-based questionnaire	Employees
[77]	To identify cyber threats in the real estate industry, assess the security awareness level of real estate employees and the risk management standards adopted by the real estate industry	Security in general	Survey-based questionnaire	Employees
[37]	To assess the risks, threats, risky assets and the on sequences of Security Breaches. To gain a deep understanding of the knowledge, attitude and behaviour related to security practices	Knowledge, Attitude, behaviour	Interview, Survey-based questionnaire	Employees
[78]	To identify critical areas of concern to address in the ICT security awareness program and the result of this assessment was used in security planning	Security manage-ment	Value-focused	Employees

Table 2.1 (continued): Previous literature on information security awareness, depicting the purpose, scope, method and target user (Adapted from [68])

Ref.	Purpose of the Study	Scope	Method	Target User
[69]	To test the proposed prototype in assessing security awareness	Knowledge, Attitude, Behaviour	Value-focused	Employees
[38]	To identify information security awareness my examining information security vulnerabilities	Knowledge, Attitude, behaviour	Value-focused, Vocabulary test	Employees
[79]	To assess the level of awareness my employing method from education discipline	Knowledge, Attitude, behaviour	Vocabulary test	Students
[80]	To examine the level of employees' experiences about their security role and management in the workplace	Security in general	Interview	Employees
[71]	To provide a rich source of users' experiences and views regarding internet security and issues of online protection	Security in general	Interview	Internet users
[81]	To identify the correct perception, myths and potential misperceptions about computer security	Security in general	Interview	Internet users
[82]	To change the behaviour and work practices of employees	Security management	E-learning	Employees
[83]	To change users' behaviour via action research	Security in general	Focus group	Employees

Table 2.1 (continued): Previous literature on information security awareness, depicting the purpose, scope, method and target user (Adapted from [68])

Ref.	Purpose of the Study	Scope	Method	Target User
[84]	To use the game technology to build stimulation systems that may help users understand information assurance concepts	Information assurance	Game	Employees
[85]	Use of hypermedia, multimedia and hypertext to provide awareness and assess security awareness among the social networking community	Security in general	Game	Social Media users
[86]	To increase awareness and enforce home users to abide by security practices while accessing online applications	Security in general	E-learning	Home users
[87]	To assess the changes in knowledge, learning and behaviour	Knowledge, behaviour	E-learning	Employees
[88]	To explore the effectiveness of the embedded training by examining the number of clicks from the spear phishing e-mail	Awareness level	Email experim-ent	Employees

Table 2.1 (continued): Previous literature on information security awareness, depicting the purpose, scope, method and target user (Adapted from [68])

2.2 Information Security Perceptions and Concerns

Perceptions are part of human intellect and have an undeniable role in fostering human behaviours [89]. Individuals evaluate external factors based on their perceptions and react to different situations. Computer and internet users respond to different kind of threats according to their perceptions. Therefore, if a person is overestimating the risks associated with threats, s/he may stop using a particular service or technology [90]–[92]. For example, people may stop using e-banking app if they overestimate the risks involved. At the same time, if a person is underestimating the risks, s/he may engage in risky behaviour and practices [93]–[95]. For example, people may share everything about their everyday life proceedings assuming they have got nothing to hide or they do not have money to lose. Thus, it is of utmost importance to understand what people perceived about information security, why they perceive what they perceive, and how they will react subsequently.

Aytes & Connolly ([96], [97]) divided users' perceptions related to information security in two groups: (1) knowledge of security risks and consequences, and (2) knowledge of security measures (also known as countermeasures). According to them, users' decision making is affected by the awareness of possible adverse outcomes and the probability of such outcomes. Moreover, awareness of safe practices, resources available to learn such practices and the cost involved in learning and employing such practices also influence their decision making. As the users are found to be the weakest link in the information security, it is essential to understand how they view information security threats, privacy threats and what are the defences they use against information security threats[16], [98].

Students are an important users' group when it comes to information security of HEIs. While online activities of students and staff members in HEIs differ, the risks of getting exposed to an information security threat may also differ [99]. It has been found that students are more exposed to security threats. To improve students' security awareness, it is crucial to understand their perceptions and concerns. This understanding will allow identifying the knowledge gaps that HEIs management may like to tackle to improve overall information security of the HEIs.

2.3 Theories in Information Security

As the user has been found as the weakest link in information security, researchers have been trying to find a way to improve their security behaviours. In this regard, researchers have made use of theories from social psychology and criminology to predict and explain users' security-related behaviours [100], [101].To have a comprehensive picture, researchers have conducted systematic reviews of the literature. For example, Lebek, Uffen, Breitner [102] conducted a review to identify the theories that have been used most often for explaining employees' information security behaviours literature. They found as many as 54 theories that have been used in information security behaviour literature. However, they found that four of the theories had been used most often. These were: Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), General Deterrence Theory (GDT), and Technology Acceptance Model (TAM). Another review conducted by Sommestad, Hallberg, Lundholm & Bengtsson [103] found that in addition to aforementioned theories, theories such as Theory of Reasoned Action (TRA) and Theory of Moral Decision Making are used in understanding information security policy compliance-related research. In this study, they found as many as 60 psychological constructs that influence policy compliance of the users. Another recent review study conducted by Mayer, Kunz & Volkamer [104] identified the 11 most reliable behavioural factors in information security contexts. However, they suggested keeping all 14 factors in mind in security behaviour related research. These factors and the respective theories are shown in **Table 2.2**.

A closer examination of existing research shows that PMT and TPB are the two most often theories used in different contexts (organisational and home-users). In both theories, security-related behaviours are predicted through behavioural intention, which is further influenced by some factors given in **Table 2.2**. Both theories are introduced in coming sub-sections.

Theory	Factors/Constructs
Theory of Planned Behaviour (TPB)	Attitude[1] Subjective Norms Self-efficacy[2] Behavioural Intention
Protection Motivation Theory (PMT)	Response Efficacy Response Costs Self-efficacy[2] Perceived Severity of threats Perceived Vulnerability Maladaptive Rewards Behavioural Intention
General Deterrence Theory (GDT)	Perceived Certainty of Sanctions Perceived Severity of Sanctions Behavioural Intention
Technology Acceptance Model (TAM)	Perceived Usefulness Perceived Ease of Use Attitude[1]

([1,2] overlapping constructs in more than one models)

Table 2.2: Reliable Behavioural Factors from Research (adapted from [104])

2.3.1 Protection Motivation Theory

Rogers proposed protection Motivation Theory (PMT) in 1975. This theory is based upon fear appeals. According to PMT, individual’s security behaviour is influenced by their beliefs about the threat and the countermeasures they can take against the threat. The beliefs about threats are termed as *threat appraisal* whereas the beliefs related to countermeasures are termed as a *coping appraisal*. Both, threat appraisal and coping appraisal, influence protection motivation (assessed as intention). Threat appraisal is measured through the severity of the threat (*Perceived Severity)* and the likelihood that a threat would occur (*Perceived Vulnerability*). The latter revolves around how effective the protective action is (*Response

Efficacy), how capable a user is of performing that action (*Self-efficacy*), and what cost the user must pay for implementing the protective action(s) (*Response Cost*). PMT posits that user's security behaviour is determined by a cost-benefit analysis where users calculate risks associated with an effort and compare them with the cost associated with the attempt to reduce the risks. The result of cost-benefit analysis motivates or demotivates (protection motivation shown as behavioural intention) a user to take precautionary measures (security behaviour). **Figure 2.2** shows the PMT model and its constituent beliefs.

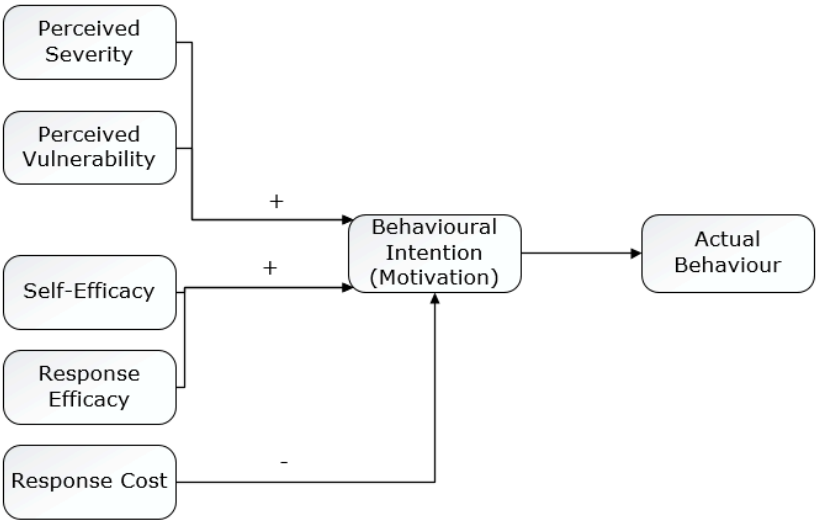


Figure 2.2: The Protection Motivation Theory, its constructs and their relationship

2.3.2 Theory of Planned Behaviour

Theory of Planned Behaviour (TPB) is evolved from the Theory of Reasoned Action (TRA) proposed by Martin Fishbein [105], [106]. TRA revolves around the *Intention* to behave in a certain way. Intention depicts the likelihood that a person will act in a particular way given the situation. The intention is predominantly influenced by the *Attitude* of the person or population towards that specific behaviour. In addition to that *Subject Norms* also affect the behaviour.

TPB was an extension of TRA where in addition to attitude and subjective norms, the concept of perceived behavioural control was introduced [107]. TPB identifies intention as the driving force for a specific behaviour which is influenced by three motivational factors: attitude, subjective norms and perceived behavioural control. The first two are the same as in TRA, while perceived behavioural control depicts the degree to which an individual thinks s/he can perform a specific behaviour. Perceived behavioural control is an important factor as even when a person has the means to act, her/his perceived inadequacy (perceived confidence in her/his capability to perform a behaviour) may prevent her/him from acting. TPB as a model is shown in **Figure 2.3**.

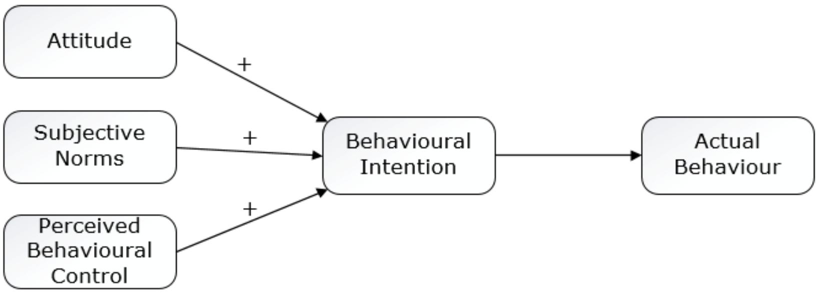


Figure 2.3: Theory of Planned Behaviour, its constructs and their relationships

2.4 Information Security Awareness and Behaviour

As discussed in the previous sections, information security awareness (ISA) is one of the important measures that could improve the security behaviours of the users. Moreover, we also saw the different behavioural factors that influence security behaviours of the users. The important thing is to understand how ISA affect security behaviours of the users.

A review of the literature showed that the relationship between ISA and security-related behaviours had been studied with the help of theories, and mostly there has been an indirect relationship between the security awareness of the behaviours. Such studies along with the context are discussed in this section.

In an organisational context, most studies are focused on awareness and behaviours related to information security policies (ISP). Al-Omari, El-Gayar & Deokar [108] used TAM to study the relationship of users' *awareness of information security, security policies, and SETA programmes* and *intention to comply with security policies* among 350 bank employees (managerial level) in Jordan*.* They found that users' awareness influence intention to comply with security policies indirectly through *perceived usefulness of protection* and *perceived ease of use (follow)* policies.

Bauer & Bernroider [109] studied and the indirect relationship of *ISA* (awareness of information security issues, risks and threats) with *ISP compliant behaviour* among 600 employees of a European bank help of Theory of Reasoned Action (TRA). They found that ISA positively affects a*ttitude* and *Social Norms* (includes both subjective and descriptive norms) which further are associated positively with the *intention to comply with ISP*. Also, the intention has a positive relationship with actual behaviour. They also found that ISA has a negative relationship with *neutralisation techniques* (the degree to which users violate ISP of the organisation due to several reasons). Neutralisation techniques are further negatively associated with intention to comply with ISP.

Bauer & Bernrodier [110] in another studied effect of ISA programs on information security compliant behaviours of bank employees using PMT. They found while there is a strong relationship ($R^2=0.56, f=0.45$) between *intention for compliant security behaviour* and *actual compliant security behaviour*, ISA programs do not affect intention directly. The impact of ISA transfers through *perceived vulnerability, perceived severity, response efficacy,* and *self-efficacy*. ISA programs, except for perceived vulnerability, have a positive relationship with other mentioned constructs. All the above-mentioned constructs have a positive relationship with intention.

Bulgurcu, Cavusoglu & Benbasat [62] conducted a study among employees (N=464) to examine the relationship of ISA with the *intention to comply with ISP* using TPB. They found that ISA affects behavioural intention through *attitude* and *perceived fairness of requirements*. ISA is positively associated with both attitude and perceived fairness of requirements. In another study [10] the same group of authors examined the relationship of ISA with beliefs about outcomes (*intrinsic benefits, safety, rewards, work impediment, intrinsic cost, vulnerability and sanctions)* and beliefs about the overall assessment of consequences (*benefit of compliance, cost of compliance and cost of non-compliance*). They further examined the relationship of the above-mentioned beliefs with the intention to comply with ISP using TPB. They suggested that ISA indirectly affect the intention to comply with ISP. ISA changes beliefs about outcomes, and these beliefs then affect beliefs about the overall assessment of consequences. Then, the beliefs about the overall assessment of consequences affect the attitude of the users. And finally, attitude affects the intention positively.

Putri & Hovav [111] conducted a study to examine the effect of ISA programs on intention to comply with ISP related to bring your own device(BYOD) among employees in Indonesia (N=230). For this purpose, they used PMT theory. They found that *BYOD security awareness programs* influence the *intention to comply with ISP* through *perceived response efficacy* and *perceived response cost*. the awareness program has a positive connection with both perceived response efficacy and perceived response cost.

Yazdanmehr & Wang [112] studied the relationship of ISP related awareness of consequence and ISP compliance behaviour using Norm Activation Theory [113]. They used a sample of working professionals in the USA (N=201). They found that ISP related awareness of consequence has an indirect relationship with IS compliance behaviour. ISP related awareness of consequence positively affects ISP-related personal norms, a combination of subjective and descriptive norms, which in turn affects the behaviour.

Torten, Reaiche & Boyle[36] studied the impact of security awareness on the security behaviour of IT professionals (N=400) in the USA using PMT. The found that threat awareness affect security behaviour through perceived severity and perceived vulnerability, whereas, countermeasures awareness affect security behaviour through self-efficacy, response cost, and response efficacy. The relationship between awareness and constructs of PMT model was positive. Study of Torten et al [36] was based upon another study [35], which was conducted to examine the relationship between ISA and security behaviour among business students (N=241). The result of this study [35] was similar to results from [36] to some extent. For example, there was a positive relationship found between threat awareness and perceived severity.

Moreover, the relationship between countermeasure awareness with self-efficacy and response efficacy was also found positive. However, there was a negative association observed in case of threat awareness-perceived vulnerability, and countermeasure awareness – response cost.

In home-users' context, Kumar, Mohan & Holowczak [114] examined the relationship between intention to use firewalls (behaviour) and awareness of security measures (ISA) with the help of TAM among 130 students who were used as a proxy for home-users. They found that *awareness of security measures* positively influence *intention to use* a firewall; however, this relationship is not direct. Awareness of security measures is positively associated with *perceived ease of use* and *perceived usefulness* which further positively affects the *Attitude* of the users. And, *Attitude* influences the intention.

Dinev & Hu [19] examined the relationship of *awareness of anti-spyware* with the *intention to use anti-spyware* a using combination of TPB and TAM using a sample of 339 university students. They found that awareness of protective technology predicts the *intention to use protective technology* both directly and indirectly. Indirectly, *awareness of protective technology* positively influences *attitude* and *subjective norm* which then predict intention. Detail of constructs/variables which are positively associated with ISA is given in **Table 2.3**, whereas, the beliefs that have a negative association with ISA are given in **Table 2.4.**

From the review, it was found that the relationship between ISA and security behaviours had been studied mostly using different models such as PMT, TPB and TAM. It was also found that in all the mentioned studies, ISA was studied as an antecedent to the models. According to Meichenbaum & Turk [115], a behaviour is operated by four independent factors: Knowledge and Skills, beliefs, motivation and action. If any of these factors are deficient, the behaviour may not as it is required. Here *knowledge and skills* refer to the necessary information of the problems, solutions, importance and self-regulatory behaviour. *Beliefs* are related to threat appraisal (perceived severity, perceived vulnerability) and coping appraisal (self-efficacy, response cost, response efficacy). *Motivation* is value and reinforcement as well as internal attribution of success. Motivation can be intrinsic or personal or extrinsic or social. And, lastly, the *actions* which are stimulated by cues, and steered by information recall. Existing theories and models used in security behaviours literature take some of these factors into account. For example, TPB takes attitude, subjective norms and self-efficacy into account which covers motivation and beliefs. PMT is based upon beliefs (coping appraisal and threat appraisal) whereas TAM and GDT also deal with the belief system. So, we need a model or theory that takes all four factors, as suggested by [115], into account.

S#	Constructs/Variables	Theory	References
1	Perceived usefulness	TAM	[108], [114]
2	Perceived ease of use	TAM	[108]
3	Attitude	TAM, TPB, PMT	[10], [19], [62], [109], [114]
4	Perceived vulnerability	PMT	[10], [36]
5	Perceived severity	PMT	[35], [36], [110]
6	Response cost	PMT	[36], [110], [111]
7	Response efficacy	PMT	[35], [36], [110], [111]
8	Self-efficacy	TPB, PMT	[35], [36]
9	Subjective norms	TPB	[19]
11	Social norms	TPB	[109]
12	Perceived sanctions (includes perceived certainty of sanctions and perceived severity of sanctions)	GDT	[10], [57], [116], [117]
13	Perceived fairness of requirements towards policies	Others	[62]
14	Intrinsic benefits	Others	[10]
15	Safety	Others	[10]
16	Rewards	Others	[10]
17	Policy-related personal norms	Others	[112]
18	Intrinsic cost	Others	[10]

Table 2.3: List of Constructs/Variables affecting Users' Security Behaviours and having positive Relationship with Information Security Awareness

S#	Constructs/Variables	Theory	References
1	Perceived vulnerability	TPB	[35], [110]
2	Response cost	TPB	[35]
3	Work Impediment	Others	[10]
4	Neutralisation Techniques	Others	[109]

Table 2.4: List of Constructs/Variables affecting Users' Security Behaviours and having negative Relationship with Information Security Awareness

2.5 Information-Motivation-Behavioural Skills Model

In 1992, Fisher & Fisher [118], [119] proposed a model to change AIDS-related risky behaviours. It covered all the four essential factors that were needed towards adherence behaviour, that is, knowledge, beliefs, motivation and actions. The model was named Information-Motivation-Behavioural Skills (IMB) Model. This model has been used in Health-related studies and showed promising results in improving behaviours [120]–[122]. IMB Model has also been used for studying voting behaviours [123] and recycling behaviours [124]. Moreover, few security researchers also proposed its utility in the context of security and privacy. However, it has not yet been tested empirically [125]–[127].

The IMB Model consists of two predictors (information and motivation), one proposed mediator variable (behavioural skills) and one outcome variable (behaviour) (**Figure 2.4**).

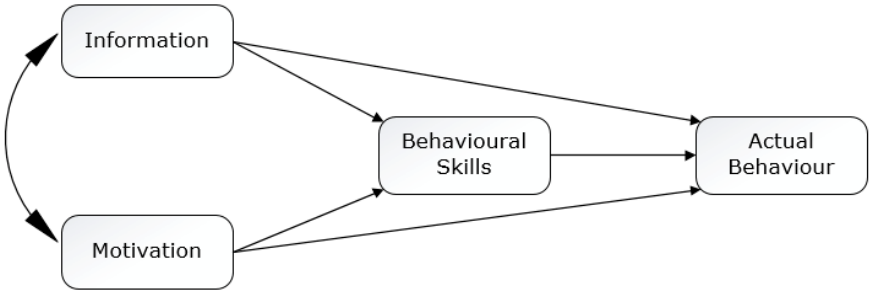


Figure 2.4: Information-Motivation-Behavioural Skills Model

2.5.1 Information

The first is information. *Information* is a prerequisite to a correct and consistent enactment of given behaviour [118], [119], [122]. In the health context, information depicts the basic knowledge of the medical condition. It may include how a disease is developed, how it progresses and the effective ways to mitigate the disease. An individual can hold accurate information (that will help in the performance of the desired behaviour) and inaccurate information (that may impede the desired behaviour).

2.5.2 Motivation

Motivation is considered a critical component for engaging in and maintaining required behaviours [128]–[130]. It is the second predictor to behaviour in the IMB model and includes both *personal* and *social motivation.* In the health context, Motivation is composed of personal attitudes towards a behaviour, and social motivation comes from the norms. The norms can be perceived social support for the behaviour, and/or the patient's perception of how others might behave in similar circumstances (descriptive norms) and perception of what others think the patient should do (subjective norms). While Fisher & Fisher [118], [119] originally considered social support as a proxy for social motivation. There has been no explicit agreement on how social motivation will be measured.

One can engage in the desired behaviour if the person is highly motivated and have a positive attitude towards the desired behaviour. Motivation may increase or decrease based on the individual's perceptions of social support to engage in specific behaviour.

2.5.3 Behavioural Skills

Behavioural skills are proposed as a mediator variable between the two predictors and security behaviour. In the health context, behavioural skills ensure that the patient has necessary skills, tools and measures or strategies to perform behaviour, for example, the patient knows how to take medicine, or use condoms. Skills include both objective and perceived abilities (self-efficacy) to deal with the challenges. Like social motivation, there is no one agreed-upon construct to measure the behavioural skills. Some considered self-efficacy as a way to measure behavioral skills [120], [131], [132], others measured with help of perceived ease of use [133], intention to perform an action related to the behaviour [134], perceived difficulty to enact a behaviour [135], and even by just by the assessment of knowledge that is needed toward enacting a behaviour [124].

Considering the usefulness of the IMB model in other contexts, and that it covers all four factors (discussed in the previous section) related to behaviour, we decided to use the IMB model to examine the relationship of ISA with the security behaviour of the students. The operationalisation of the constructs is discussed in Chapter 6.

2.6 Summary

In this chapter, a review of existing literature related to this thesis has been provided. The chapter starts with providing an understanding of ISA as a concept, followed by a synthesis of existing studies on ISA highlighting the purpose, scope, method and respondents of those study. Importance of perceptions and concern is also discussed. I have also provided an overview of most often used theories in information security behaviour research followed by an introduction of IMB Model. In next chapter, we will describe the relationship of different individual factors with ISA of the students.

Chapter 3

Assessment of Information Security Awareness among Students

This chapter presents a user study to assess and relate information security awareness of 614 Finnish university students with their demographic factors to identify the student groups which lack security awareness. This study relates to ***O*₁** of the thesis.

The importance of information assets has been widely accepted, and companies spend huge capital on information security to ensure business continuity and disaster recovery [14], [136]. For this purpose, usually a security plan is designed wherein not only common technical tools and solutions are considered, but the focus is given to the human factor as well; sole focus on technological solutions is not an answer to the problem[137]–[139]. People are trained and educated so that they have sufficient knowledge of security threats and their role in the whole security scenario[140]. The literature suggests information security policies, security education, training and awareness programs[10]–[12], [58] for educating people. The significance of information security awareness (ISA) has been acknowledged by the researchers not only in the previous century [13], [14], [141], [142] but also in recent times, and several studies have focused on ISA (for example, [48], [54], [69], [79], [143]).

The use of Internet-based information systems and related services such as online social networks among the students is on the rise amid rapid growth in the technology, introduction of online courses and digital libraries [144], [145]. Research shows that the educational institutions, especially universities, have been hot targets for cybercriminals due to two main reasons; 1) vast computing power and 2) open access to the public and its constituencies [146]. The importance of information security in the context of educational institutes has been recognised, and Educause Review [147] has ranked it number one or number two among areas of concerns for educational institutions in the USA over last several years. Although the importance of ISA in educational institutions is increasing, the studies related to ISA in the context of educational institutions are scarce, and those available are focused on issues other than students' ISA assessment and training. The issues focused on the available studies are the adoption of information security in higher education institutions [148], assessing employees' ISA [149] and information security strategies [150]. However, ISA in context of students was discussed while providing guidelines and recommendations for ISA training for college students [144]. Because most of ISA related studies related to students were conducted in the USA, Australia, and that in most of the cases students from one or two backgrounds (disciplines) were subjects of the studies, we decided to conduct an ISA assessment among students from different backgrounds.

In this regard, we, first, examined the relationship of demographics (such as gender, age, educational background), cultural factors (nationality, the area of living), and individual factors (job experience and previous ISA training) with students' perceived as well as actual ISA. Here perceived ISA (termed as PISA in this chapter) was the subjective measure of students' ISA and was directly measured from the respondents on a 5-point scale (1: very low to 5: very high), whereas, actual ISA (termed as AISA) was a combination of knowledge and behaviour test score (objective knowledge and competency-based questions) of the students. In this regard, we employed a *t*-test, Pearson's correlation and *one-way ANOVA with* posthoc, depending upon the type of independent variables (individual cultural, job experience and previous ISA training). A cross-section survey was conducted to collect data on variables described above for students of seven faculties of the University of Turku, Finland. Information security awareness, security awareness and ISA have been used interchangeably in this chapter.

The rest of the chapter is organised as follows: In section 3.2 we discuss related work on ISA. Section 3.3 describes the methodology used in the study, followed by Results and Discussion in Section 3.4. Section 3.5 provides our concluding remarks and future recommendations.

3.1 Related Work

Information is defined as a resource, commodity, perception of pattern and constitutive force in our lives [151]. Information has some characteristics that make it valuable to its owner and its intended users. Some believe that confidentiality, integrity and availability are the important characteristics that should be fortified [152], whereas, for others availability, accuracy, authenticity, confidentiality, integrity, utility and its possession are the important characteristics of information [153]. However, in any case, information security ensures that the information is not accessed, used, disclosed, disrupted, modified, seen, recorded or destructed by an unauthorised entity [154]. To improve information security, ISA has been suggested as a tool by researchers [62], [86]. In literature, ISA has been conceptualised differently in different contexts and this diversity at times frustrates information security researchers, practitioners and security managers [155]. Some believe ISA is only seeking and directing the attention of individuals to information security and that they should be concerned about it [156]–[158], while others believe that it is not just a matter of directing, but it is also ensuring compliance of the individuals [48].

There are several studies related to ISA assessment targeting the general public and the employees of organisations. These studies include both proprietary[159], [160] and academic with specific objectives. For example, Herath & Rao [161] discussed the role of penalties, pressures and perceived effectiveness in enhancing ISA in an organisation, Stanton et al. [162] conducted a survey-based passwords related behavioural study, focused on mobile computing, Furnell et al. [137] assess users' view of security features within different applications and Siponen, Pahnila, & Mahmood [163] studied information security policy related normative beliefs and intentions. All these studies have used different methods for assessing ISA. Since our context was higher education institutions, it was not deemed appropriate to use any of the methods used in the studies mentioned above. At the time of this study, there were students of 84 different nationalities studying at undergraduate and postgraduate degree programs in eight different faculties of our target university. Therefore, a questionnaire was required that should be easily understandable by the students from different educational and cultural backgrounds. Education, ISA related training and working experience are considered as intervening factors and demographics as individual factors while designing a human element of information security model [38]. This model has been developed keeping in view the employees of an organisation, whereas, in our case, the target population was university students. In another study, the roles of mother tongue and area of living in ISA of students are assessed [164]. As the first step in our investigation, we decided to examine the direct relationship of factors such as age, gender, nationality, educational level, field of study, area of living, working experience and information security-related training to ISA and its constituent dimensions, knowledge and behaviour. In this paper, we call such factors as individual factors.

Furthermore, our perusal of literature revealed that no single method fits all situations. However, the vocabulary test [79] was found most appropriate for our study. Like Kruger et al.'s work [79], we also considered knowledge and behaviour as two dimensions of ISA. Knowledge is an essential element in the cognitive learning process [165]. Perceived knowledge may not be the same as actual knowledge, but it shows how confident users feel regarding a phenomenon. According to [70], cognitive, metacognitive, affective, conative and cross-cultural factors impact personal learning. The cognitive factor refers to acquiring and implementation of the knowledge. In [165], it is suggested that there are three cognitive skills necessary for effective learning experience; (1) knowledge of facts, processes and concepts (2) ability to apply the knowledge (3) ability to reason. So if a person has sufficient knowledge of a concept she/he can use that knowledge. Kruger & Kearney[69] argue that if a person is not aware of the basic concepts of information security, s/he is more prone to information security threats than the others.

3.2 Methodology of ISA Assessment

3.2.1 Objective of Study

The objective of this study was to examine information security awareness among university student. For this purpose, two variables were defined to understand ISA:

1) Perceived ISA which explains the subjective measure of ISA among the students (denoted as PISA in this study)

2) Actual ISA which depicts the objective measure of awareness (denoted as AISA in this chapter)

PISA was directly measured from the respondents whereas, AISA was computed by taking mean of knowledge and behaviour scores a respondent got after answering knowledge and competency-based questions depicting behaviour. Next, the respondents were divided into groups based on their demographics, cultural factors and individual factor and examined the differences in perceived ISA, knowledge, behaviour and attained ISA among those groups.

3.2.2 Research Questions and Hypothesis

Following are the research questions of the study:

RQ$_1$: What is the overall security awareness level among the students?

RQ$_2$: Who has better in security awareness among the students if divided based upon their demographics, cultural and individual factors?

RQ$_3$: What are the common sources of security awareness among the students?

To answer *RQ$_2$* following hypothesis are created:

H1: *There is no gender difference in knowledge, behaviour, and security awareness (perceived and actual) among the students*

H2: *There is no difference in knowledge, behaviour, and security awareness (perceived and actual) among the students due to the age difference.*

H3: *There is no difference in knowledge, behaviour, and security awareness (perceived and actual) among the students from a different educational level.*

H4: *There is no difference in knowledge, behaviour, and security awareness (perceived and actual) among the students from different educational discipline.*

H5: *There is no difference in knowledge, behaviour, and security awareness (perceived and actual) between Finnish and international students.*

H6: *There is no difference in knowledge, behaviour, and security awareness (perceived and actual) among students coming from rural, urban and metropolitan backgrounds.*

H7: *There is no difference in knowledge, behaviour, and security awareness (perceived and actual) between students having ISA training previously and students without any training.*

H8: *There is no difference in knowledge, behaviour, and security awareness (perceived and actual) between students having working experience and students having no working experience.*

3.2.3 Survey Design

A simple descriptive case study survey design was adopted for this study. This design was deemed suitable as it allows the researcher to identify the characteristics of the population by asking a question(s) without studying the whole population. At the same time, it will enable the collection of a large amount of data within the particular case [166].

3.2.4 The Instrument

A questionnaire was developed based on previous work [79], [167]. However, additional questions were added keeping in mind the target audience. While structuring the questionnaire, the principles of survey methodology suggested by Dillman (2011) were kept in mind. The full questionnaire is available at **Appendix-A**. Here the structure of the questionnaire is succinctly described.

There were three major parts of the questionnaire. Part 1 consisted of categorical questions related to age, gender, working experience, educational discipline, educational level, ISA training, country of origin and type of living area before joining the existing university. Measurement scales are described later in Section 3.3.6 (Data Analysis).

A question was added to record the PISA of the respondents. PISA was measured on a 6-point Likert scale (1: very low to 5: very high, 6: unsure). Another question asking about preferred sources of information security awareness was also asked. The respondents could select one option from the academic material, family & friends, informal discussion with peers, formal training, newspaper or magazine, and websites & search engines.

Part 2 of the questionnaire consisted of 10 multiple choice questions that tested the objective knowledge of the respondents regarding different threats and security incidents. The threats include worms, Trojan horses, spam, social engineering, phishing, pharming, botnets, denial of service attacks, zero-day attacks and security incidents. **Snippet 3.1** shows an example of a vocabulary test for the term spam.

Spam is:

a) Another word for e-mail or electronic messages
b) A marketing technique
c) Any unsolicited electronic mail
d) All of the above
e) I do not know what spam is
f) I did not understand the question due to language

Snippet 3.1: Knowledge test example for Spam

It was expected that someone with a good understanding of the concept of spam would select option 'c' as the most appropriate answer. Unlike the work of Kruger et al. [79], we added the 6th option, which could be selected if the responder is unable to understand the question due to the language barrier. This question was added as English is not an official language in Finland and it was speculated that there could be issues due to language. However, there were only 12 respondents who selected this option for some questions and hence their responses were excluded from data analysis.

Part 3 of the questionnaire consisted of 10 scenario and competency-based questions aimed at the testing behaviour of the students against the threats mentioned in Part 2 as well as incident handling, information sharing habits in online social networks, email practices and password management practices. **Snippet 3.2** shows a question, as an example, that was used to test behaviour for password management. According to Mansfield [169], behavioural questions are used as an effective way to discover an individual's behaviour in a quick and precise manner. However, most of the behavioural questions are scale-based and are prone to social desirability bias. To overcome this bias, we used scenario-based and competency-based questions.

The instrument validity was checked through a content validation and reliability test. Once the questionnaire was designed, an expert penal consisting of three persons having a background in information security and psychology examined the questionnaire for its content validity. Also, the successful use of a similar instrument in previous work by other researchers supports the content validity [79], [167]. Reliability of the instrument was measured through the Cronbach alpha coefficient, the value of which was found acceptable (0.61).

Once a password is allotted for your university's email account, you do the following: (Select One most suitable)

a) I never change my default password
b) I change it when the system asks me to change it
c) I usually change it
d) I always change it

Snippet 3.2: Behaviour Test example for "Password Management."

3.2.5 Data Collection

The questionnaire was uploaded online using Google Docs, and the link to the survey was forwarded to educational program coordinators in different faculties. Every faculty has its student mailing list, in which email addresses of all the students are added at the time of registration and removed upon the completion of their studies. The program coordinators then forwarded the questionnaire's link along with an introductory statement to these mailing lists. In this way, the questionnaire link reached all the registered students in the university. At the time of this survey, there were 17069 students enrolled at undergraduate and postgraduate level (female: 60,19%, International students: 11,52%) [170]. The data collection process continued for 22 days during January 2013, and as a result, a sample of 614 usable responses was collected. The response rate from different faculties is shown in **Table 3.1.**

3.2.6 Data Analysis

After the data collection, data analysis was conducted to find out answers to the research questions. Statistical Package for Social Sciences (SPSS 25.0) was used for this purpose. Data was first coded into numerical form for the analysis in SPSS.

For analysis, as a first step, knowledge and behaviour scores were calculated. Each correct answer to knowledge and behaviour questions were coded as 1, whereas, a wrong answer was coded as 0. In certain cases, response to a knowledge and behaviour question was partially correct. In such cases, responses were coded as 0.5. So, the theoretical range of knowledge and behaviour scores was between 1 and 10. To compute actual security awareness (AISA), we took mean of the knowledge and behaviour scores. The theoretical range of AISA was also between 1 and 10. The theoretical range of PISA was between 0 and 5. Following scale was used for interpretation of knowledge, behaviour and AISA: 0-2 = very low, >2-4=low, >4-6=average, >6-8=high, >8-10=very high. The statistical tests used for testing hypothesis are shown in **Table 3.2.**

Disciplines	Population	Sample	Response
Economics	3060	65	2.12%
Education	1969	77	3.91%
Humanities	3960	142	3.59%
Law	1165	17	1.46%
Medicine	1768	68	3.85%
Mathematics & Natural Sciences	3478	203	5.84%
Social Sciences	1669	42	2.52%
Total	**17069**	**614**	**3.60%**

Table 3.1: Student population at the time of the survey

Variable Name	Variable Type	Test Used
Gender	Nominal (dichotomous)	t-test
Age	Nominal (multi-group)	ANOVA
Educational Level	Nominal (multi-group)	ANOVA
Nationality	Nominal (dichotomous)	t-test
Area of Living	Nominal (multi-group)	ANOVA
ISA Training	Nominal (dichotomous)	t-test
Working Experience	Nominal (dichotomous)	t-test

Table 3.2: Statistical test used for analysis

3.3 Results and Discussion

Table 3.3 shows the complete sample characteristics. Most of the respondents were female (57 %), which was in line with the overall population: females constituted 60 % of the target population at the time of the study. 23.50 % of the respondents were international students, while at the time of this survey they made up 11.52 % of the total student population at the university. Most respondents (46.90 %) came from urban areas of living such as big towns and small cities. Surprisingly, the response rate from the bachelor's and master's students was equal and constituted the major portion of the sample (96.40 %). Overall, the lowest response rate was recorded from the students of law and social science, whereas, the highest number of respondents were from the humanities and information technology (IT). Around one fourth (24.30%) of the respondents have undergone information security related training in the past. Almost half of the students (52.60%) have full time or part time working experience in their field of studies.

Factors	Sample (n=614)	Population (N=17069)
Gender		
Female	57 %	60.10%
Male	43 %	39.90%
Age		+
Under 21	9.90 %	
21-25	48.00 %	
26-30	29.50 %	
31-40	9.40 %	
41-50	2.10 %	
Above 50	1.00 %	
Education level		
Bachelor	48.20 %	58.15%
Master	48.20 %	31.21%
Doctoral	3.60 %	10.64%
Nationality		
Local (Finnish)	76.50 %	88.48%
International	23.50 %	11.52%

*(*IT student's population is included in Other Natural Sciences.*
+ data for the population is not available.)

Table 3.3: Sample Statistics of respondents for ISA study

Factors	Sample (n=614)	Population (N=17069)
Discipline		
Economics	10.60 %	17.93%
Education	12.50 %	11.54%
Humanities	23.10 %	23.20%
Information Technology (IT)	17.30 %	*
Law	2.80 %	6.83%
Medicine	11.10 %	10.36%
Other Natural Sciences	15.80 %	20.38%
Social Sciences	6.80 %	9.78%
Living Area		+
Rural (Small town)	33.22 %	
Urban (Big Town/small Cities)	46.90 %	
Metropolitan (Big Cities)	19.87 %	
Training		+
Yes	24.30 %	
No	75.70 %	
Experience		+
Yes	52.60 %	
No	47.50 %	

(+ data for the population is not available.)

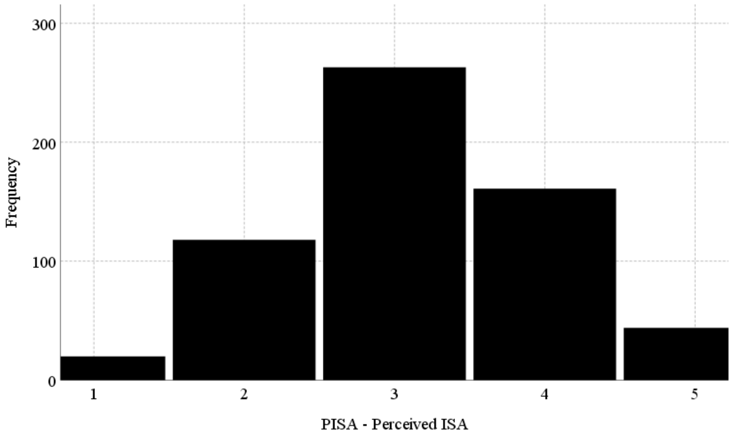
Table 3.3 (continued): Sample Statistics of respondents for ISA study

3.3.1 Overall Awareness

Frequency distributions of PISA, knowledge, behaviour, and AISA were computed to have an overall assessment of knowledge, behaviour and awareness, and are shown in **Figures 3.1 to Figure 3.4** respectively.

Examination of the frequency distribution of PISA showed that the actual range of PISA scores was the same as a theoretical range (that is between 1 and 5). About half of respondents (43%) believed that they had an average level (3) of ISA. 23% of the respondents thought that they had at least low PISA (1: very low, 2: low). Around 26% and 7% of the respondents believed that they had a high (4) and very high level (5) of PISA, respectively (for the frequency distribution of PISA consult **Figure 3.1)**. The mean of PISA was 3.15 with an

SD of 0.92 (Min:1, Max:5). There were only 1% of respondents who were unsure about their security awareness level.



(1: very low, 5: very high)

Figure 3.1: Frequency distribution of respondents' PISA

The frequency distribution for knowledge score is shown in **Figure 3.2**. Both theoretical range and the actual range of knowledge score were between 1 and 10. About 13% of the respondents had very low, 34% had low, 26% had an average, 22% had high, and only 5% had very high-level security knowledge. 1.6% of the respondent scored 0. The most occurring scores were 3 (10%), whereas, the least occurring score was 10 (0.50%). The mean score for knowledge was 4.72 with SD: 2.21 (Min:0, Max:10).

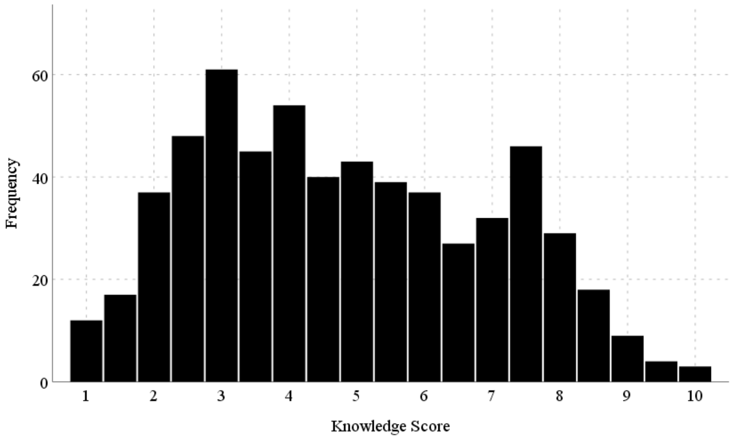


Figure 3.2: Frequency distribution of respondents' knowledge score (theoretical range 1-10)

Like knowledge score, the behaviour score had a theoretical range of 1 to 10. However, the actual range was found to be between 1.5 and 9.5 (consult **Figure 3.3**). About 4% of respondents were of low level, 46% were average, 45% were high, and 4% were very high regarding security behaviour. Less than 1% of respondents scored very low for behavioural test scores. The most occurring score was 6(14.80%), whereas the least occurring score was 1(0.20%). The mean for behaviour score was 6.23 with SD:1.22 (Min:0, Max:10).

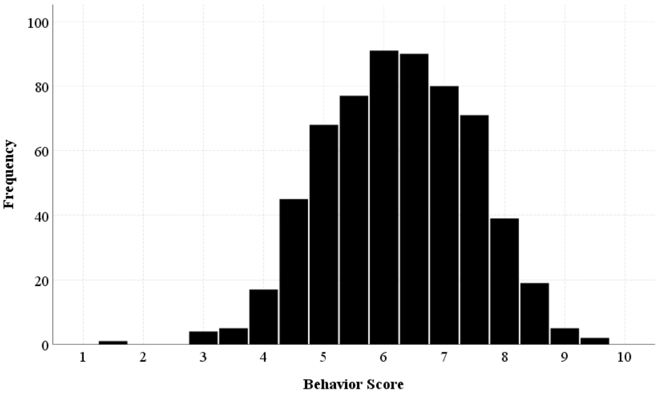


Figure 3.3: Frequency distribution of respondents' behaviour score (theoretical range: 1-10)

AISA was computed by taking the mean of the knowledge and behaviour score, and thus, AISA's theoretical range was also between 1 and 10. In AISA, 16% of the respondents scored low, 51% scored average, 30% scored high, and only 3% scored very high. The most occurring score was 5 and 5.25 (about 8% each), whereas, the least occurring score was 2.25 and 9 (0.20% each). For frequency distribution consult **Figure 3.4**. The mean AISA score was 5.48 with SD:1.36 (Min:0, Max:10).

Based on the above results, we can conclude that most respondents perceived to have average or higher security awareness. Regarding objective knowledge, about half of the respondents (53%) score average or higher. In the behavioural test, respondents had a better score as compared to the objective measure of knowledge. 95% of the respondents had an average or higher score for the behaviour. In actual ISA, which is a combination of knowledge and behaviour, 84% of the respondents were average or higher regarding security awareness.

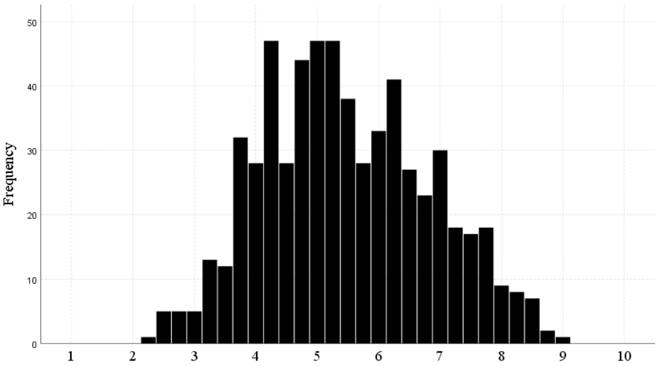


Figure 3.4: Frequency distribution of respondents' AISA *(theoretical range: 1-10; AISA mean score on x-axis)*

3.3.2 Gender Differences

To examine gender differences in PISA, knowledge, behaviour and AISA, we ran a series of t-tests. The results for gender-differences are shown in **Table 3.4**.

Table 3.4 shows that males were found to be better regarding information security knowledge, behaviour, PISA and AISA. The differences were statistically significant (at $p<0.001$) in all the cases. Thus, our hypothesis (*H1*) could not be supported, as there is a significant difference in knowledge, behaviour and awareness (perceived and actual) between male and female students.

Variables	**Male (N=264)**		**Female (N=350)**		***t***	***p****
	M	**SD**	**M**	**SD**		
PISA	3.53	0.96	2.86	0.79	9.071	*<0,001*
Knowledge	5.79	2.14	3.91	1.90	11.246	*<0,001*
Behaviour	6.43	1.23	6.07	1.19	3.664	*<0,001*
AISA	6.11	1.32	4.99	1.17	10.868	*<0,001*

(at p<0.05)*

Table 3.4: t-test statistics showing gender differences in PISA, knowledge, behaviour and AISA

3.3.3 Differences due to Age

The age of the respondents was measured in 6 groups: Under 21, 21-25, 26-30, 31-40, 40-50 and Above 50. Table 3.3 shows that some respondents in "40 and above" groups were very few (about 3%) and thus removed from the analysis. We compared students of four groups only. ANOVA was run to ascertain if there are differences among the different groups, whereas, a post-hoc test was also employed to pinpoint where exactly the difference is coming. The descriptive, as well as ANOVA statistics, are shown in **Table 3.5.** From the table, we can conclude that there is a statistically significant difference in knowledge and perceived awareness (PISA) among student belonging to different age groups, however, no difference was found in case of behaviour or actual awareness (AISA).

Variables	**Age Group**	**N**	**Mean**	**SD**	***f***	***p****
PISA	U 21	60	2.95	0.77	3.358	*0.019*
	21-25	290	3.08	0.90		
	26-30	179	3.26	0.95		
	31-40	58	3.36	1.07		
	Total	587	3.15	0.92		
Knowledge	U 21	61	4.11	2.21	3.474	*0.016*
	21-25	295	4.65	2.22		
	26-30	181	5.02	2.13		
	31-40	58	5.15	2.35		
	Total	595	4.76	2.22		
Behaviour	U 21	61	6.10	1.12	0.742	0.528
	21-25	295	6.27	1.20		
	26-30	181	6.22	1.20		
	31-40	58	6.05	1.34		
	Total	595	6.22	1.21		
AISA	U 21	61	5.11	1.27	2.402	0.067
	21-25	295	5.46	1.37		
	26-30	181	5.62	1.32		
	31-40	58	5.60	1.43		
	Total	595	5.49	1.35		

($p<0.05$)*

Table 3.5: ANOVA statistics showing differences in PISA, knowledge, behaviour and AISA due to age

In **Table 3.5**, we can see that there is a significant difference in perceived awareness (PISA) between the groups (*F (3, 3.583) = 3.358, p=0.019*). An LSD post hoc test revealed that "under 21" students significantly differ in PISA from students of age group "26-30" (Mean difference=-0.313, p=0.02), and students of age group "31-40" (Mean difference=-0.412, p=0.016). No significant difference was found between students of "under 21" and "21-25" age groups. Moreover, students of age group "21-25" significantly differ from students of age group "26-30" (Mean difference=-0.180, p=0.04), and students of age group "31-40" (Mean difference=-0.279, p=0.03). The difference between students with age group "26-30" and "31-40" was statistically insignificant. So, we can conclude that students of age "under 21 to 25" were different in perceived awareness from students of age group "26-40".

The difference of knowledge among the groups was also found significantly different (*F (3, 3.591) = 3.474, p=0.016*). An LSD post hoc test showed that "under 21" students were significantly different in knowledge from students of age group "26-30" (Mean difference: -0.91, p=0.005) and students of age group "31-40" (Mean difference: -1.04, p=0.01). No significant difference was found between students of age group "under 21" and "21-25". Moreover, students belonging to age groups 21-25, 26-30 and 31-40 were not different from one another regarding knowledge. No significant differences were found among students of the different age group in behaviour or AISA.

Based upon above results, we may conclude that students, if divided into age groups (under 21, 21-25, 26-30 and 31-40), differ significantly in PISA and knowledge and not in behaviour or AISA. Younger students (age under 21 to 25) perceived to have significantly lesser awareness (PISA) as compared to older students (age 26 to 40). Regarding knowledge, the younger students (aged under 21) found to have lesser security knowledge as compared to elder groups (21 to 40).

3.3.4 Difference due to Educational Level

As shown in **Table 3.3**, students' educational level was measured regarding their class: Bachelor, masters and doctoral. However, for the sake of analysis students of master and doctoral levels were merged and two groups: undergraduate and post-graduate were created. a t-test was employed to test the hypothesis. The results from the t-test are shown in **Table 3.6**.

Variables	**Undergraduate (N=296)**		**Post-graduate (N=318)**		***t***	***p***
	M	**SD**	**M**	**SD**		
PISA	3.13	0.87	3.16	0.98	-0.398	0.69
Knowledge	4.59	2.16	4.84	2.25	-1.434	0.15
Behaviour	6.26	1.23	6.20	1.21	0.597	0.55
AISA	5.42	1.34	5.52	1.37	-0.900	0.36

(p<0.05)*

Table 3.6: t-statistics showing differences in PISA, knowledge, behaviour and AISA due to educational level

From the results in **Table 3.6**, we can see that our hypothesis *H3* is supported, that is, there is no difference in knowledge, behaviour, perceived and actual awareness due to educational level.

3.3.5 Differences due to Educational Disciplines

As shown in **Table 3.3,** students from eight faculties responded to the survey. However, the number of responses was not uniform across the disciplines. Among the respondents, 6.80% belonged to social sciences whereas only 2.80% belonged to the law faculty. Because we were applying ANOVA test, a small sub-sample may not yield any important results and, therefore, we did not include students from social sciences and law in the ANOVA test. The results of the ANOVA test are shown in **Table 3.7**.

Based upon statistics given in **Table 3.7**, hypothesis *H4* is rejected, as there are significant differences in knowledge *(F(5, 549)= 31.008, p<0.001))*, behaviour *(F(5, 549)=2.906, p=0.013))*, PISA *(F(5, 541)= 13.908, p<0.001))* and AISA *(F(5, 549)= 26.446, p<0.001))*) among the students belonging to different disciplines.

The highest PISA was found among IT students (Mean:3.79, SD:0.89). The difference in PISA was significantly different from PISA of students from other disciplines at *p<0.05*

(IT>Economics=Medicine>NaturalSci.>Humanities>Education). PISA was not found statistically significantly different among students of other disciplines.

Variables	Disciplines	N	Mean	*f*	*p*
PISA	Economics	65	3.09	13.908	*<0.001*
	Education	76	2.84		
	Humanities	139	3.02		
	IT	105	3.79		
	Medicine	67	3.09		
	Natural Sci.	95	3.03		
	Total	547	3.16		
Knowledge	Economics	65	4.90	31.008	*<0.001*
	Education	77	3.56		
	Humanities	142	4.19		
	IT	106	6.77		
	Medicine	68	4.41		
	Natural Sci.	97	4.75		
	Total	555	4.80		
Behaviour	Economics	65	5.97	2.906	*0.013*
	Education	77	6.09		
	Humanities	142	6.15		
	IT	106	6.60		
	Medicine	68	6.16		
	Natural Sci.	97	6.26		
	Total	555	6.23		
AISA	Economics	65	5.44	26,446	*<0.001*
	Education	77	4.82		
	Humanities	142	5.18		
	IT	106	6.69		
	Medicine	68	5.29		
	Natural Sci.	97	5.50		
	Total	555	5.52		

(p<0.05)*

Table 3.7: ANOVA statistics showing differences in PISA, knowledge, behaviour and AISA due to educational discipline

The knowledge score for IT students was also found significantly higher (*Mean difference ranges from 1.86 to 3.20)* than students from other disciplines (at *p<0.05)*. However, in the case of knowledge, a statistically significant difference in mean score was also found between economics and education students *(Mean difference: 1.34, p<0.01)*, economics and humanities students *(Mean difference: 0.71, p=0.016)*, Education and humanities students *(Mean difference: -0.63, p=0.02),* Education and medicine students *(Mean difference: -0.84, p=0.01)* and humanities and natural sciences students *(Mean difference: -0.55, p<0.01).*

Like knowledge scores, the behaviour score of IT students was also found significantly higher than the rest of the students (*Mean difference ranges from 0.34 to 0.63 at p<0.05)*. However, no statistically significant difference in behaviour was found among students from other disciplines.

IT students were also found better than students from other disciplines in actual awareness (AISA) (*Mean difference ranges from 1.18 to 1.86, at p<0.05*). Among other disciplines, students of economics were found different from education students (*Mean difference=0.61, p=0.003*). Education students were also found different from humanities (*Mean difference = -0.35, p=0.046*), medicine (*Mean difference=-0.46, p=0.026*) and natural sciences students (*Mean difference=-0.68, p<0.01*). Moreover, students of Humanities were found different from natural sciences students (*Mean difference=-0.33, p=0.044*).

In short, there was a statistically significant difference in PISA, knowledge, behaviour and AIA of students from a different discipline. The difference was mainly because of the high scores of IT students in all four variables. However, regarding knowledge differences were found among students of other subjects as well.

3.3.6 Differences due to Country of Origin

Our case university is an international country where students of different nationalities are studying in various disciplines. To examine, if there is a difference of knowledge, behaviour, perceived and actual awareness in local and international students, a t-test was run. The results from the *t-test* are shown in **Table 3.8**.

Based on results given in **Table 3.8**, it can be concluded that there was only a statistically significant difference in case of behaviour *(p<0.05)*. No statistically significant difference in PISA, knowledge and AISA of local and international students*.*

Variables	Local (N=470)		International (N=144)		*t*	*p*
	M	SD	M	SD		
PISA	3.19	0.89	3.02	1.02	1.897	0.06
Knowledge	4.72	2.20	4.72	2.27	-0.042	0.97
Behaviour	6.29	1.23	6.05	1.15	2.014	0.04
AISA	5.50	1.37	5.39	1.31	0.870	0.39

(p<0.05)*

Table 3.8: T-statistics showing differences in PISA, knowledge, behaviour and AISA due to the country of origin

3.3.7 Differences due to Area of Living

In addition to country of origin, students were also asked to provide information on the type of area they had been living at the time of schooling before joining the current university. They could select one option from "rural", "urban" and "metropolitan". To examine the difference in knowledge, behaviour, perceived and attained behaviour that may arise due to the difference in areas of living, ANOVA test was conducted. The results of the ANOVA test are shown in **Table 3.9.**

The results of the ANOVA test show that no significant difference in knowledge, behaviour, perceived and actual awareness was found among students coming from rural, urban or metropolitan areas *(significance at p<0.05)*. Therefore, we accept our hypothesis *H6.*

3.3.7 Differences due to Previous Training

To ascertain if a previous ISA related training affects knowledge, behaviour, perceived and actual awareness of the students, we ran an independent sample t-test. The groups were: students who have previously undergone ISA related training and students who have not undergone any ISA related training. The results of the t-test are shown in **Table 3.10**. The t-statistics show that students who previously had ISA training were better regarding knowledge, behaviour, perceived and actual awareness, and the difference between training and untrained students was statistically significant. Therefore, hypothesis *H7* was rejected.

Variables	Area	N	M	SD	*f*	*p*
PISA	Rural	202	3.12	0.88	1.978	0,139
	Urban	284	3.11	0.91		
	Metro.	120	3.30	1.04		
	Total	606	3.15	0.93		
Knowledge	Rural	204	4.53	2.21	2.829	0.060
	Urban	288	4.68	2.15		
	Metro.	122	5.13	2.33		
	Total	614	4.72	2.22		
Behavior	Rural	204	6.20	1.30	1.1330	0.265
	Urban	288	6.31	1.19		
	Metro.	122	6.10	1.17		
	Total	614	6.23	1.22		
AISA	Rural	204	5.37	1.39	2.366	0.278
	Urban	288	5.50	1.31		
	Metro.	122	5.61	1.42		
	Total	614	5.48	1.36		

(p<0.05)*

Table 3.9: ANOVA statistics showing differences in PISA, knowledge, behaviour and AISA due to the area of living

Variables	Trained (N=149)		Untrained (N=465)		*t*	*p*
	M	SD	M	SD		
PISA	3.78	0.87	2.95	0.85	-10.274	<0.01
Knowledge	6.15	2.08	4.26	2.05	-9.706	<0.01
Behaviour	6.45	1.25	6.15	1.20	-2.593	<0.01
AISA	6.30	1.34	5.21	1.25	-9.090	<0.01

(p<0.05)*

Table 3.10: t-statistics showing differences in PISA, knowledge, behaviour and AISA due to previous ISA training

3.3.8 Differences due to Work Experience

University students usually work along with their studies, especially international students. Since organisations have information security mechanism emplaced, it is highly likely that a student who is doing a job has got some information security awareness at his/her job place. To ascertain if there is a difference of knowledge, behaviour, perceived and actual security awareness among students who are working beside their studies, and the ones who do not work, we ran a t-test. The results of the t-test are shown in **Table 3.11**.

The t-statistics show that students who were employed along with their studies were different from the students who were not employed in case of PISA only. In other cases, no significant difference was found. Since it was not asked what type of jobs was done by the students, it is difficult to ascertain if students have information security-related training at their workplaces.

Variables	**Employed (N=323)**		**Unemployed (N=286)**		***t***	***p***
	M	**SD**	**M**	**SD**		
PISA	3.23	0.94	3.06	0.90	2.288	0.023
Knowledge	4.86	2.27	4.57	2.14	1.577	0.115
Behaviour	6.19	1.24	6.28	1.19	-0.872	0.382
AISA	5.52	1.41	5.42	1.29	0.896	0.370

(p<0.05)*

Table 3.11: T-statistics showing differences in PISA, knowledge, behaviour and AISA due to work experience

3.3.9 Preferred Sources of Awareness

We observed from the results of the study that there were significant differences in perceived ISA, knowledge, behaviour and actual ISA due to gender and educational discipline and previously taken ISA training. It was found that male was better than female students; IT students were better than non-IT students and already trained students were better than untrained students, it would be interesting to see if there is the difference in preferred sources of ISA among the student from different backgrounds. The respondents were also asked to mention the sources from where they have gained some form of ISA. **Figure 3.5** shows students’ preferences of sources of ISA in percentage.

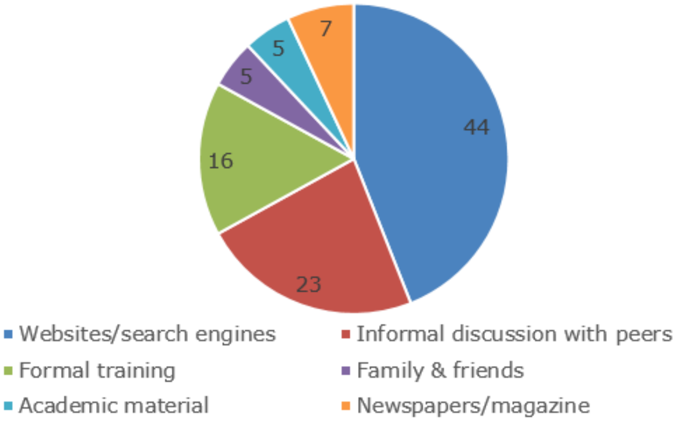


Figure 3.5: Preferred Sources of Security Awareness among the Students (in percentage).

Application of the chi-square test was performed to explore the relationship between gender, educational discipline and Trained/untrained students. Educational disciplines were divided into two groups: IT vs Non-IT.

The relationship between gender and preferred source of ISA was found statistically significant, X^2*(5, N=319) = 21.247, p=0.001*. More male than female students (57% vs 34%) prefer to learn ISA from websites and search engines, whereas, more female than male students (29% vs 16%) prefer to learn through informal discussions with the peers.

Moreover, the relationship between educational discipline (IT vs Non-IT) and preferred source of ISA was also statistically significant, X^2*(5, N=319) = 20.102, p=0.001.* More IT students than Non-IT students (14% vs 3%) prefer to learn ISA from academic sources such as books, journals.

Lastly, the relationship between previous ISA training and preferred source of ISA was also found statistically significant, X^2*(5, N=319) = 20.858, p=0.00*. A further examination showed that more untrained students than trained students (26% vs 15%) prefer to learn ISA through informal discussions with peers.

3.3.10 Relationship of Perceived and Actual Awareness

Since we collected data to examine perceived as well as the actual awareness, it was decided to examine the relationship of perceived security awareness with knowledge, behaviour and the actual security awareness. For this purpose, we ran a Pearson's correlation tests and examined scatter plots. The relationship between PISA and knowledge, PISA and behaviour and PISA and AISA are shown in **Figure 3.6, 3.7** and **3.8** respectively. In the figures, the dotted lines depict mean confidence interval. The value of correlation coefficient (*r)*, significance (*p)* and the coefficient of determination (*R^2*) in each case are also given in the caption of the figures.

In **Figure 3.6**, we can see there is a positive relationship between perceived security awareness and security knowledge. The strength of association was moderate but significant (r=0.50, p<0.05). It means as the PISA of students increases (from very low to very high), the security knowledge of students also increases (from very low to very high). So, we can see that the students who perceived to have high perceived security awareness, had a high level of security knowledge. In this regard, 24% of the variance in knowledge is explained by perceived security awareness of the users (*R^2=0.24)*.

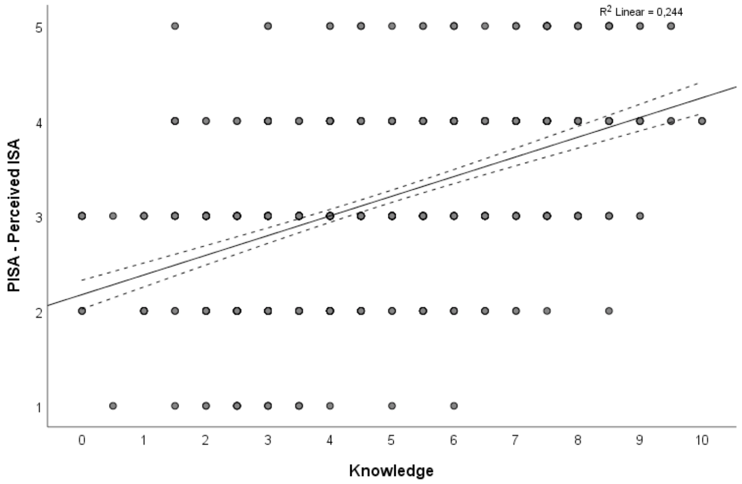


Figure 3.6: Relationship between Perceived Security Awareness and Security Knowledge (*r=0.50, p<0.05, R^2=0.24)*

In the case of behaviour, the correlation between PISA and behaviour was found to be positive as well. However, the relationship was weak but significant (r=0.13, p=0.002). From the correlation coefficient, we can say that students having high perceived security awareness had better security behaviour.

However, the weak correlation suggests that the relationship between the variables above is weak. In other words, a student having high perceived security awareness may not behave securely as compared to students having low perceived security awareness. The scatterplot showing the relationship between perceived security awareness and security behaviour is shown in **Figure 3.7.**

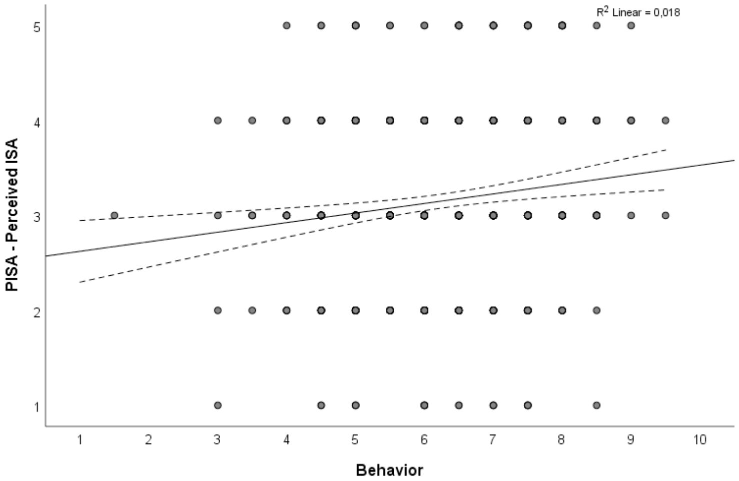


Figure 3.7: Relationship between Perceived Security Awareness and Security Behaviour (*r=0.13, p=0.002, R^2=0.02)*

The relationship between perceived security awareness and actual security awareness was found to significant (at p<0.05). The correlation was moderate (r=0.46), whereas, 21% of the variance in actual security awareness could be explained by the perceived security awareness. The scatter plot showing the relationship between perceived and actual security awareness is shown in **Figure 3.8.** This relationship indicates that the students who have high perceived security awareness have a high actual security awareness. It is pertinent to mention that since actual security awareness is a combination of knowledge and behaviour, probably it is the knowledge score that is the reason behind a high level of association.

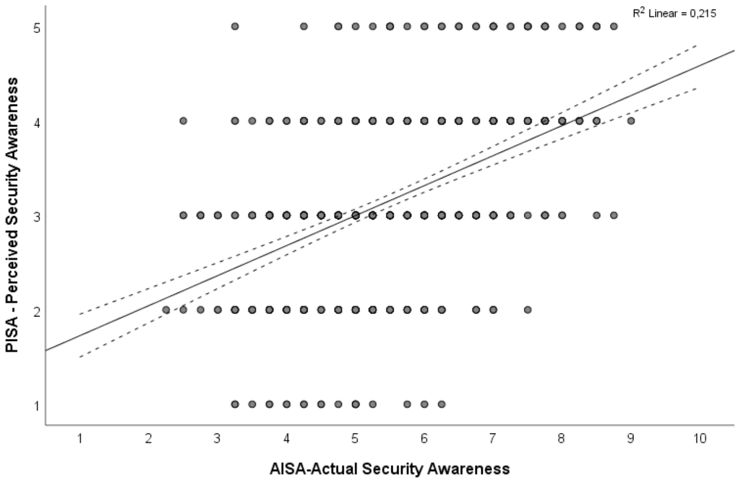


Figure 3.8: Relationship between Perceived Security Awareness and Actual Security Awareness (*r=0.46, p<0.05, R²=0.21)*

3.4 Summary

In this chapter, we have presented the result of a study assessing Information Security Awareness (ISA) among the students in a multicultural, multidisciplinary Finnish university. The study was conducted using a questionnaire where 614 valid responses were collected from all the seven faculties of the target university. The target was to get a general understanding of ISA and to examine the relationship of different factors such as age, gender, educational level, disciplines, nationality, the area of living, working experience and information security training may impact ISA. In the study, ISA was measured both subjectively (Perceived security awareness) and objectively (actual security awareness). The actual security awareness consisted of two dimensions: security knowledge and security behaviour. Perceived security awareness was directly measured from the respondents on a 5-point scale, whereas, the actual security awareness was mean of the knowledge and behaviour scores respondents received in the knowledge and behavioural test (questionnaire).

In general, the measured knowledge correlated with security behaviour *(r=0.18, p<0.05)*, but the actual impact was surprisingly low. Although the actual behaviour is difficult to measure using a questionnaire due to social desirability bias, we tried to minimise this bias by using scenario-based questions measuring behaviour. During the analysis, we found that

perceived security awareness correlates with security knowledge, security behaviour and actual security awareness of the respondents. While these relationships were statistically significant, perceived security awareness explained significant variance in security knowledge *(R^2=0.24)* and actual security awareness *(R^2=0.21)*. So, we can assume that users considered perceived security awareness as a proxy of security knowledge. However, the same may not be right for the actual security awareness, as in our case, actual security awareness was a combination of security knowledge and security behaviour and thus the correlation of perceived and actual security awareness maybe because to moderate correlation between perceived security awareness and security knowledge.

Overall, the majority (76%) of the students perceived to average or higher security awareness, whereas a large portion (47%) of respondents scored a low score in the knowledge testing. On the opposite, only 4% of the respondents had low scores in behaviour testing. From this we may conclude that perhaps students were not aware of the threats. However, they have learnt specific security-related behaviours from different sources and adopted as it is.

Among the demographics, gender had a substantial impact on ISA. Overall, the male students got better scores than the female ones, especially in the knowledge part. Age-wise, the younger students (under the age of 25) perceived to have lesser security awareness, whereas knowledge-wise students of age 21 and below had less knowledge of security threats as compared to older students. No difference in security behaviour or actual security awareness was found due to age. Quite surprising no differences in perceived or actual security awareness (including security knowledge and behaviours) were observed due to the difference in educational level. The effect of the educational discipline in question was surprisingly low. The only exception was information technology (IT) students who performed better than the rest.

To examine the impact of cultural diversity on ISA, we used two proxy variables: nationality and area of living. On average, Finnish students received a bit higher scores than international students. However, the only significant difference was in case of security behaviours. This result was impacted by the fact that the number of international students was the highest in the IT Discipline. In many faculties, international students are in practice non-existent. Further, no difference in perceived or actual security awareness was found among students who came from a rural, urban or metropolitan background.

Previous security awareness training was found to be another variable which has a substantial impact on the perceived and actual security awareness after gender. The students who had a security awareness training were found to be significantly better than untrained students in all the four variables under study. Highest impact was seen perceive security awareness and security knowledge. Moreover, working experience impacted only to perceive security awareness.

Lastly, websites and search engines were found to be the most preferred source for security awareness among the students. However, there have been some differences in preferences among male and female students, IT and non-IT students, and previously trained and untrained students. Websites and search engines were the most preferred source of security awareness among the male students, whereas, female students prefer to learn through informal discussions with their peers. IT students prefer to learn from academic materials such as books and journals. And, the students who did not have any security-related training prefer to learn from informal discussions, just like female students.

In next chapter, a sequential mixed method study for identifying students’ security concerns have been presented.

Chapter 4

Identification of Students' Information Security Concerns: A Sequential Exploratory Study

In the previous chapter, we examined relationship of different factors with perceived awareness, actual awareness and security behaviour of the students. This chapter describes a two-phased study wherein using a mixed method sequential design, identifying students' concerns related to their information security and unveiled the areas where students perceived to have information security risks. This chapter is related to ***O_2*** of the thesis.

Humans are often considered as the weakest link in security [5]. It has been found the time and again that adequate information security is not possible only by implementing technical measures and requires the users to be mindful of security threats and measures. A variety of technical [9] and non-technical measures [11], [12], [58], [62] have been suggested to safeguard organisational and individual security. However, users often fail to take the necessary measures and actions [97]. Organisations invest heavily on their information security. For example, organisations have security policies in place, have dedicated staff looking after information security issues, and management employ variety of "stick and carrot" tactics, such are awareness training, incentives, monitoring and deterrence approach to motivate employees [171]. However, home-users or users who are not employed do not have the same facilities or resources and, thus, make decisions by themselves. While existing security literature has been predominantly focussed on organisational context [171], [172], security researchers have turned their focus to home-users [172]. In recent years, some studies have been published focussing on the information security of the home-users, for example, [98], [173]–[175].

Like in any other organisation, information security is one of the concerns for the educational institutions [176]. Information security has been ranked as one of the top areas of concerns for educational institutions in the United States [147]. The availability of vast amounts of computing power and open access has attracted the attention of malicious entities towards higher educational institutions (HEIs) [146] (HEIs are referred as institutions imparting post-secondary education, such as universities and colleges). However, HEIs are considered to have inadequate protection regarding the security of their information assets [26].

A variety of technical [9] and non-technical measures [11], [12], [58], [62] have been suggested to safeguard organisational and individual security. Security education, training, and awareness (SETA) programs are suggested as a tool to improve information security awareness of the users [144]. ISA has been considered as one of the defences against continuously evolving threat landscape, and a way to mitigate security attacks [54], [177]–[179]. Information security awareness (ISA) enables a user to understand his role in the security process and encourages her/him to take necessary measures for his, as well as his peers, information security [54], [155]. The importance of ISA is similar for a different type of users, be it employees of an organisation [37], [180], or home users [86], [98], or the students [73], [144], [181].

According to the Concerns-based Adoption Model (CBAM) [182], having a concern is first to step towards change and to learn new behaviour. If a person is concerned about a phenomenon, s/he will try to get awareness about it leading to a stage where he will be able to adopt the change or learn the required skill. Keeping in view the importance of ISA, researchers have studied the concept thoroughly, including its antecedents as well as the consequences [34]. However, in most of the available studies, security experts identify an area where ISA is to be assessed and improved, based upon their expert knowledge, and end-users (employees, home-users, students) are involved in the assessment phase. Research shows that perceptions of threats play an important role toward (in)action of the end-users that would ensure or endanger the information security of users [183]. Users have different mental models related to information security threats [184], and resultantly threats are perceived differently. Therefore, we suggest that end-users' concerns be taken into consideration at the time of identifying areas where ISA is to be assessed and improved. If we can understand the users' security concerns, their prevalence and variation, the whole ISA process can be improved.

In this regard, a two-phase study was conducted to explore students' perceptions of information security threats systematically. In doing so, in the first phase, opinions on perceived security threats and countermeasures were collected from a group of forty-two master's IT degree students. Using an inductive approach and content analysis seventy-four different concerns related to information were identified. In the second phase, a diverse group of students belonging to different educational backgrounds were asked to rate those concerns. Factor analysis was used to examine the underlying structure of the concerns. We found that students' information security concerns can be divided into 11 factors, each depicting an area of concern. These areas are related to personal, social, institutional, technological and non-technological aspects of students' lives.

Rest of the chapter is organised as follow: Section 4.2 provides the importance of information security awareness among the students, followed by a review of current studies on information security of students in Section 4.3. Section 4.4 narrates the methodology used in the study. Findings from the first and second phases are given in Section 4.5 and 4.6 respectively. The conclusion is given in Section 4.7.

4.1 Information Security Awareness and Students

Like in any other organisation, information security is one of the concerns for the educational institutions [176]. Information security has been ranked as one of the top areas of concerns for educational institutions in the United States [147]. The availability of vast amounts of computing power and open access has attracted the attention of malicious entities towards higher educational institutions (HEIs) [146]. HEIs, university, institution and educational institutions have been used in this paper, all referring to institutions imparting post-secondary education (bachelor's level and above). However, HEIs are considered to have inadequate protection regarding the security of their information assets [26]. To up-lift the information security defences of the HEIs, it is essential that both employees and students exhibit secure behaviour.

Students make a large portion of HEIs and are at high risk and attractive candidates for information security attacks [185]. Students are a peculiar set of internet users. Students are although one sub-set of internet users groups, however, their access and usage of internet and computer may be dissimilar to other sub-groups such as non-home users (NHU) and home-users (HU) [86]. NHU are employees of an organisation and mostly access the internet and computers from their workplace. NHU's use of the Internet is usually under a watchful eye of IT and security staff to ensure nothing is being done outside rules and regulations of the organisation, including information security.

On the other hand, HU does not have any such oversight guaranteeing their information security. In a typical setting, some users share characteristics of a HU as well as NHU [86]. Students fall into a similar category (**Figure 4.1**). Like any organisation, end-users' of HEIs (employees and students) are provided with security tools and instructions and warned about the security issues. However, university management does not have the same level of control over students' security practices as they have in case of employees [186].

In the quest for comprehensive security for HEI, a multi-layered security approach is required where users are required to take more than one measure to safeguard their information security [187]. Missing one or more measures will leave the loophole in the defence. Therefore, an insecure behaviour on the part of students can expose them, their peers, and their HEIs to a variety of information security threats. Moreover, they are going to be work-force to different organisations. If they continue with their insecure behaviour, it will eventually create troubles for the organisations as well.

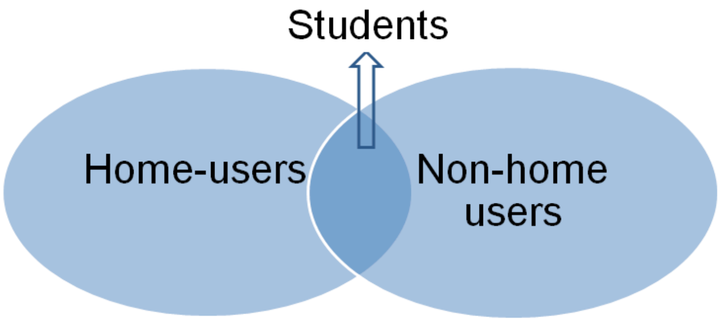


Figure 4.1: Home-users (HU), Non-Home Users (NHU) and Students (Adapted from [86])

4.2 Current Studies on Information Security of Students

While literature is full of studies focusing on the information security of NHU, HU has also caught the eyes of the researchers. However, security issues of students, who have been used as proxies for both HU and NHU in the literature quite often, has not been examined as thoroughly as other user groups (For the definitions of NHU and HU, please consult previous). The researchers have studied ISA of students in isolation, that is, within one component or area such as password-related behaviour [162], application security in computers [137] or smartphone security [188]; while others took a more holistic approach where more than one components/areas were used for assessing ISA [38], [189]. There is a need to identify a set of areas related to the day-to-day life of users where their information security can be jeopardised. Such areas then combined with areas identified by the security experts can provide a comprehensive set of areas where ISA of the users can be improved.

The use of computers and the internet is probably more pervasive among students than the other two sub-groups. Students use computers and the internet for a wide range of activities including accessing emails, completing educational activities, performing financial transactions and socialising [190]. Like other internet users, also students' information security is also at risk due to evolving information security threats. Students learn information security knowledge from a variety of sources such as websites and search engines, formal training, informal discussions with their peers, books and journals [181].

Examination of existing literature on information security of students highlights the areas where, in security experts' opinion, students' information security is at risk. These areas include system security, email practices, password practices, threats/attacks knowledge, institutional policies, data security and privacy, cloud services, online social networks, network security, web/internet browsing, information sharing, device security, and mobile phones (refer to **Table 4.1** for detail). The areas above are not mentioned as areas in all these studies. However, the areas are depicted by the statements and items used to study perceptions, knowledge, practices and behaviours of the users.

From the review of the literature, we found that there was only one study where students' perception was examined by collecting data directly from the students using interviews [191]. Otherwise, in all other studies, students were given statements regarding particular action (practices/ behaviours) and asked to respond on the ordinal or categorical scale. In the identified studies, the security experts/researchers identified the areas and actions within those areas and later on, students gave their opinions.

Areas	Action Studied and References
System Security	Antivirus use/installation/updating and the frequency of scan; Ad blocker; Firewall use; Intrusion detection system use; computer security tools use; OS/software update; Patches and updates; anti-spyware use; UPS use; Password use; log off behaviour; pen drive scanning [74], [144], [174], [186], [192]–[202]
Email Practices	Opening email from an unknown sender; reporting suspicious email; opening attachments from an unknown sender; opening attachments without scanning; open non-suspicious email from strangers; opening interesting emails without concern; verifying sender before opening an attachment; use of a password on attachment; clicking on unknown email links; scanning email attachments before opening; delete suspicious emails without reading [144], [174], [193]–[195], [198], [201], [202]
Threat/ Knowledge	Knowledge concepts (worms, Trojan horse, spam, social engineering, phishing, pharming, botnets, denial of service attack, zero-day attack, security incidents) [73], [191], [193], [199], [203]–[207]
Services	Using cloud apps; awareness of security and privacy issues in cloud computing [74], [199]
Passwords	writing down password; sharing passwords; using of the multifaceted authentication system; changing passwords frequently/regularly; emailing passwords; strong password characteristics; using different passwords on different systems; password management practices (changing default password, changing with system asks, usually change it, always change); keeping password secret; creating passwords not easy to guess(strong passwords) [73], [144], [174], [193], [195]–[197], [201], [202], [204]–[206], [208], [209]

Table 4.1: Existing Studies on Students’ Information Security

Areas	Action Studied and References
Policies	Opinion on college policy (password length, complexity, changing and reusability); Awareness of university's policy on (safeguarding passwords, virus protection, VPN, authentication on a university network) [193], [209]
Data	Use of encryption; taking backups; frequency of taking backups; data privacy; knowing risk of peer-to-peer file sharing [73], [74], [192], [196]–[198], [206], [209], [210]
Online Social Networks	Risk acceptance in giving up privacy against convenience; impact awareness of giving up privacy against convenience; awareness of risk from the reduction of privacy for increased convenience; awareness of information breaches [74], [199]
Network	Awareness of WiFi security [192]
Web Browsing	Risk awareness of downloading random programs or files; use of pop-up blocker; awareness of unsafe website [144], [194], [209]
Device	Awareness of personal devices, textbooks security; anti-theft/fraud; pen drive scanning [196], [211]
Smart Phone	Harmful behaviour; protection through add-on and mobile phone settings; disaster recovery; viruses; use of anti-virus; knowledge of encryption; enabling sim pin code; screen password, Bluetooth disable; phone sharing; not saving passwords on the phone; not saving personal data on the phone; software update; installing third-party software; responding to email/SMS [73], [206], [210], [212], [213]
Info sharing	Sharing credentials online [196], [207]

Table 4.1 (Continued): Existing Studies on Students' Information Security

4.3 Methodology for Identifying Concerns

4.3.1 Research Question

The purpose of this study was to identify information security concerns of the students and to examine if there is a difference in concerns among students from different backgrounds. Following questions were defined for the study:

> ***RQ: What are information security concerns among the students in HEI context?***

4.3.2 Study Design

End user's point of view can be gathered using qualitative or quantitative methods. However, rather than using either qualitative or quantitative approach, data from the students were collected and analysed using both qualitative and quantitative approaches. The mixed method approach provided us with rather rich data for the analysis. A sequential mixed method design consisting of two phases (qualitative and quantitative) was used for data collection and analysis.

With the help of this design, we first collected the data from a group of forty-two master's degree IT security students enrolled in a course focused on the human element in information security, using open-ended question. The qualitative approach allowed the researchers to gather rich and detailed explanations of complex phenomena and help in revealing the context [214]. Data collected through such approaches also provide an understanding of the experiences, the attitudes and, aims at answering "what?" questions about a phenomenon [215]. Researchers often use a group of field experts to identify different issues within a domain, for example, Kraemer, Carayon, & Clem [216] used the same methodology to identify and describe human and organisational factors related to computer and information security. However, since we wanted to keep this study free from expert opinion, we selected a group of master's degree IT security students. Master's degree IT security students are trained in the security and privacy domain, and soon they are supposed to assume responsibilities as security professionals. Thus, we assumed that master's degree IT students would have better knowledge of information security and privacy threats as compared to other disciplines. Two researchers in information security examined the collected data. The examination resulted in identifying seventy-four students' perceived threats and vulnerabilities, hereafter called concerns.

In the second phase, a survey was conducted among students of higher education to ascertain if the identified concerns were valid for a broader population of the students. The students were recruited from a multidisciplinary Finnish University. Views of four hundred and seventeen students (N=417) were collected in this regard. The collected data was checked for the quality and reduced to a usable sample of N=354. The usable sample was then analysed using the descriptive statistics (mean, median, mode and standard deviations). Principal Component Analysis using principal axis factoring with oblique rotation was used to identify underlying factors in the data [217]. These factors depicted the focus areas where students perceived to have information security concerns. In this way, we identified 14 focus areas. The sequential study design, showing the phases, the procedure and the outputs, is shown in **Figure 4.2**.

4.3.3 Material and Method

In the second phase, an online survey was sent to students of a Finnish University situated in a southwestern province of Finland during January 2017. The invitation to participation was shared using different mediums such as notice boards and distribution through faculty members. We did not use the mailing lists of the university as we conducted another survey in the recent past and it was envisaged that inviting students to another study might not catch the attention of the students. There was no benefit, monetary or otherwise, offered to survey participants. 417 responses were collected until September 2017. However, after removing the incomplete responses and the responses depicting response bias, we were left with a usable sample of 354 respondents. The survey took 25-30 minute on an average.

The questionnaire for this phase was developed using the list of concerns identified in the first phase. The students were asked to rate these concerns against the statement "How concerned you are for…" on a 7-point scale (1: not at all concern to 7: extremely concerned). Another option (I don't know) was added so that if a respondent is not aware of stated issue s/he could select it. The final survey included 74 Likert scale items and five items measuring gender, educational level, discipline, and previous information security related training (categorical) and age (continuous).

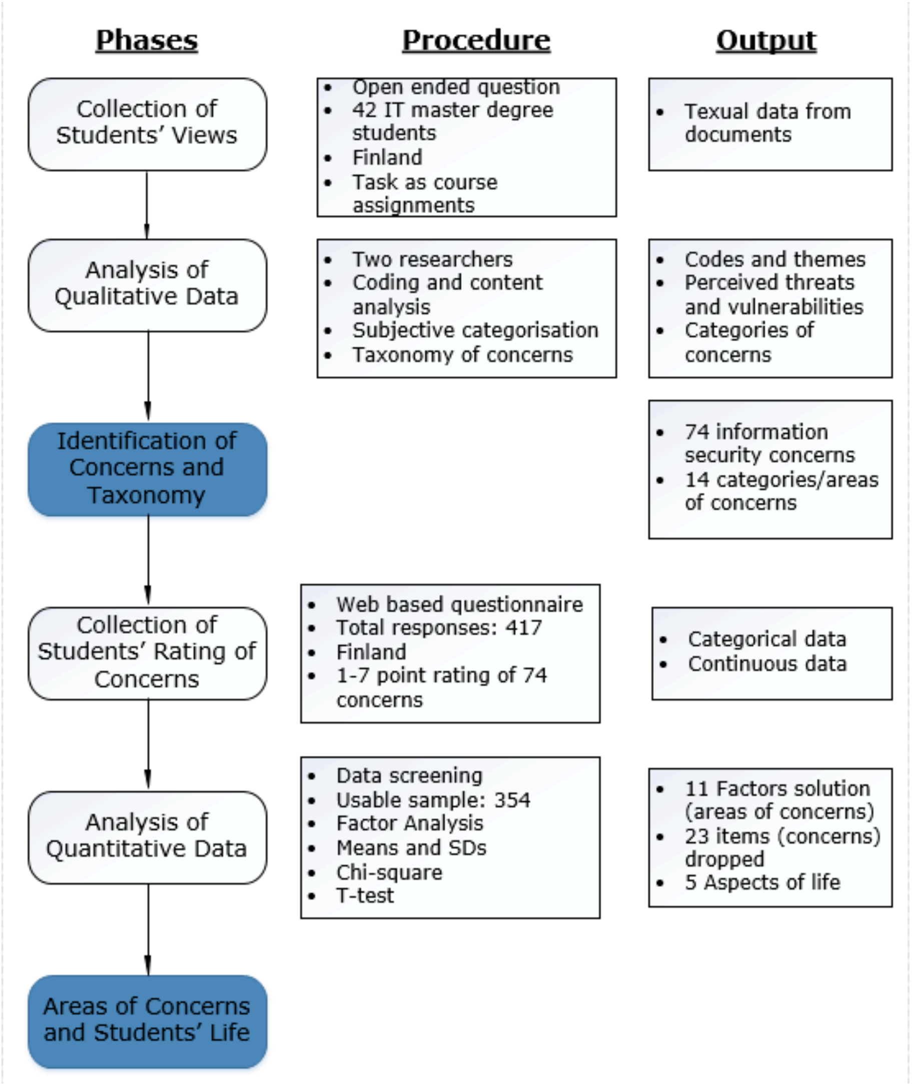

Phases
Procedure
Output
Collection of Students' Views
Open ended question
42 IT master degree students
Finland
Task as course assignments
Texual data from documents
Analysis of Qualitative Data
Two researchers
Coding and content analysis
Subjective categorisation
Taxonomy of concerns
Codes and themes
Perceived threats and vulnerabilities
Categories of concerns
Identification of Concerns and Taxonomy
74 information security concerns
14 categories/areas of concerns
Collection of Students' Rating of Concerns
Web based questionnaire
Total responses: 417
Finland
1-7 point rating of 74 concerns
Categorical data
Continuous data
Analysis of Quantitative Data
Data screening
Usable sample: 354
Factor Analysis
Means and SDs
Chi-square
T-test
11 Factors solution (areas of concerns)
23 items (concerns) dropped
5 Aspects of life
Areas of Concerns and Students' Life

Figure 4.2: Sequential Study Design explaining Phases, Procedures and Products

4.3.4 Data Analysis

This qualitative data was collected from 42 Master 's degree IT security students (male=39, Female=3) during March-April 2015. The collected data were analysed using the content analysis technique.

Two researchers coded the concerns and grouped them based upon the functional areas. Here functional area is a synonym to the focus area. Following rules were adopted during the examination:

1) The threats will be examined concerning the function and/or service is at risk. For example, one of the students mentioned that "…Also, some unintentional personal details can be sent to the wrong email if for example an automatic signature in use." Since the threat was related to emails, we put it in functional area "emails".

2) The threats related to the same function and/or service will be put into one category.

3) The threat will be put into the relevant category based upon cause but not the effect. For example, the participants mentioned that weak passwords for payment services are a threat to students' IS&P. So, the cause is the weak password and not the payment service, and hence this threat was categorised into category "Passwords" and not into "Online Services".

Once the content analysis had been done by the experts separately, they sat together and cross-checked the extracted concerns and the categories. After discussions and deliberations, seventy-five identified perceived threats were put into fourteen categories. Each category was constructed keeping in view the principles of classification [218]. The categories were given meaningful names based on the function and service. List of concerns along with the categories is available at **Table 4.2.**

S#	Category	Code	Concern
1	Web Access	WA1	Click Jacking
2		WA2	Local browser history and search history
3		WA3	Local storage of password in the browser
4		WA4	Ads and malware embedded in websites
5		WA5	Unwanted backend downloads
6		WA6	Cheap and free online services
7	Proximity and Interaction	PnI1	Unintentional data disclosure during presentation on projector
8		PnI2	Shoulder surfing in classroom
9		PnI3	Shoulder surfing in a cafeteria
10		PnI4	Lending devices to Friends
11		PnI5	Lending Devices to Family
12		PnI6	Misuse of personal data by boy/girlfriend
13		PnI7	ID theft due to group work
14	Personal Belongings	PB1	Theft/Loss of Student ID
15		PB2	Theft/Loss of banking cards
16		PB3	Theft of wallet
17		PB4	Theft/Loss of multipurpose Student card
18	Personal Electronic Devices	PED1	Theft/Loss of PEDs
19		PED2	Malware and Virus in PEDs
20		PED3	Over-reliance on antivirus suites in PEDs
21		PED4	Use of pirated software and apps in PEDs
22		PED5	Ransomware in PEDs
23		PED6	Loss of device due to natural calamity
24		PED7	Loss of unencrypted flash drive

Table 4.2: List of Students' Information Security Concerns grouped by the Researchers

S#	Category	Code	Concern
25	Student Information System	SIS1	Study record leakage because of cyber-attack
26		*SIS2*	*Data loss from student's information system due to natural calamity*
27	Smart phones	SP1	Theft/Loss of smartphone
28		SP2	Malware/Infected Apps in smartphones
29		SP3	Weaker security/pin codes for banking apps
30		SP4	GPS Photo metadata in smartphones
31		SP5	Unauthorised Bluetooth/Wi-Fi connection to smartphones
32		SP6	Location disclosure services in smart phones
33		SP7	Apps access to phone content
34		SP8	Periodic vendor's data backups in smartphones
35	Policy Issues	PI1	Improper disposal of students' data
36		PI2	Inadequacy of school's privacy policies
37	Network Administration	NA1	Access to the history of students' activity online by IT Staff
38		NA2	IT staff access to students' profile data
39	University Communication Networks	UCN1	Unauthorised access to university login
40		UCN2	Malware and virus from shared media
41		UCN3	Insecure wireless networks at University
42		UCN4	Hardware skimmers and keyloggers at university workstations
43		UCN5	Cyberattack on University network
44		UCN6	Use of online banking on the university network
45		UCN7	Compromised university workstation
46		UCN8	Leaving workstation unlocked/without logging off
47		UCN9	VPN access to infected machine to university network

Table 4.2 (continued): List of Students' Information Security Concerns grouped by the Researchers

S#	Category	Code	Concern
48	Emailing	EM1	Malware and virus through emails
49		EM2	Spam through emails
50		EM3	Emails Signature shared with the unintended recipient
51		EM4	Phishing/Targeted Phishing through emails
52	Online Services	OS1	Search String collection and targeted advertisement
53		OS2	Data leakage from cloud services
54		OS3	Excessive data collection by service providers
55	Passwords	PW1	Reuse/one password multiple accounts
56		PW2	Single Sign-On
57		PW3	Weak passwords
58		PW4	Brute force attack
59		PW5	Weak passcodes for payment services
60	Online Social Networks	OSN1	Phishing attack on the online social network
61		OSN2	Malware and virus in social networks
62		OSN3	Inter-platform connectivity among social networks
63		OSN4	Scam messages in social networks
64		OSN5	Hacking in social networks
65		OSN6	Excessive Information Sharing in social networks
66		OSN7	Info sharing by others in social media (SM)
67		OSN8	Family tree leakage in social networks
68		OSN9	ID theft in social networks

Table 4.2 (continued): List of Students' Information Security Concerns grouped by the Researchers

S#	Category	Code	Concern
69	Other Concerns	OC1	Ignorance of local cyber laws
70		OC2	Bugs in software and hardware
71		OC3	Unintentional release of student's info by the teacher
72		OC4	Carelessness towards reading terms and conditions
73		OC5	Government access to individual data
74		OC6	University staff's negligence toward students' data

Table 4.2 (continued): List of Students' Information Security Concerns grouped by the Researchers

The data (N=354) collected during Phase-2 was analysed using IBM's Statistical analysis software package, SPSS (version 25). The sample characteristics of the sample used in phase 2 are given in **Table 4.3.**

Variables	Characteristics	%
Gender	Female	54.20
	Male	45.80
Age group	<21	26.60
	21-25	68.40
	>26	5.10
Educational Level	Bachelor (UG)	65.00
	Masters (PG)	35.00
Educational Discipline	Economics	34.20
	Education	12.40
	Humanities	2.50
	IT/CS/Engineering	28.80
	Medicine	1.10
	Natural Sciences	19.50
	Social Sciences	1.40
Previous Training	Yes	30.00
	No	70.00

Table 4.3: Sample Characteristics of participants (Phase-2)

In the qualitative phase, we identified security concerns of the IT security students and grouped them based on the subjective judgement of the researchers. To understand the security concerns of students from a diverse background, we asked 417 students to rate their concern level for the identified concerns on a 7-point scale. Unlike the first step, we ran a factor analysis to uncover the underlying factors of the concerns. In this regard, PCA was used. PCA is an established technique used for deducing factors robust to correlation and has been extensively used in psychology and human-computer interaction literature [219]–[222]. PCA was conducted using principal axis factoring with the oblique rotation, as recommended by [217].

Initially, we identified 14 factors using the Kaiser Criterion, having eigenvalues greater than 1 [223], allowing item loading greater than 0,4, explaining a total variance (TVE) of 69.90%. We repeated the same step by removing items having loadings less than 0,4; no or few item cross-loadings; items; items with cross loading difference more than 0.15 or loading heavily (0.40) on more than one factors were removed; and, items loading on the different components measure different constructs. Haywood cases were removed (item loading higher than 1.0). We also kept in mind the face validity of the factors, that is, similar items should be loaded under one factor, and if not, such items were removed. Once the final eight factors were reduced after a couple of iterations, we observed that one of the factors contains items each explaining three different concepts. At this point, to minimise the data loss, we relaxed our criteria (no fewer than three items per factor) and divided the factor into three factors explaining three different concepts. In this way, we came up with a solution consisting of 11 reliable and stable factors, explaining 68.87% of the variance (Kaiser-Meyer-Olkin Measure of Sampling Adequacy:0.946, Bartlett's Test of Sphericity: 13580.86, df:1275, p<0.001).

4.4 Results of Qualitative Study

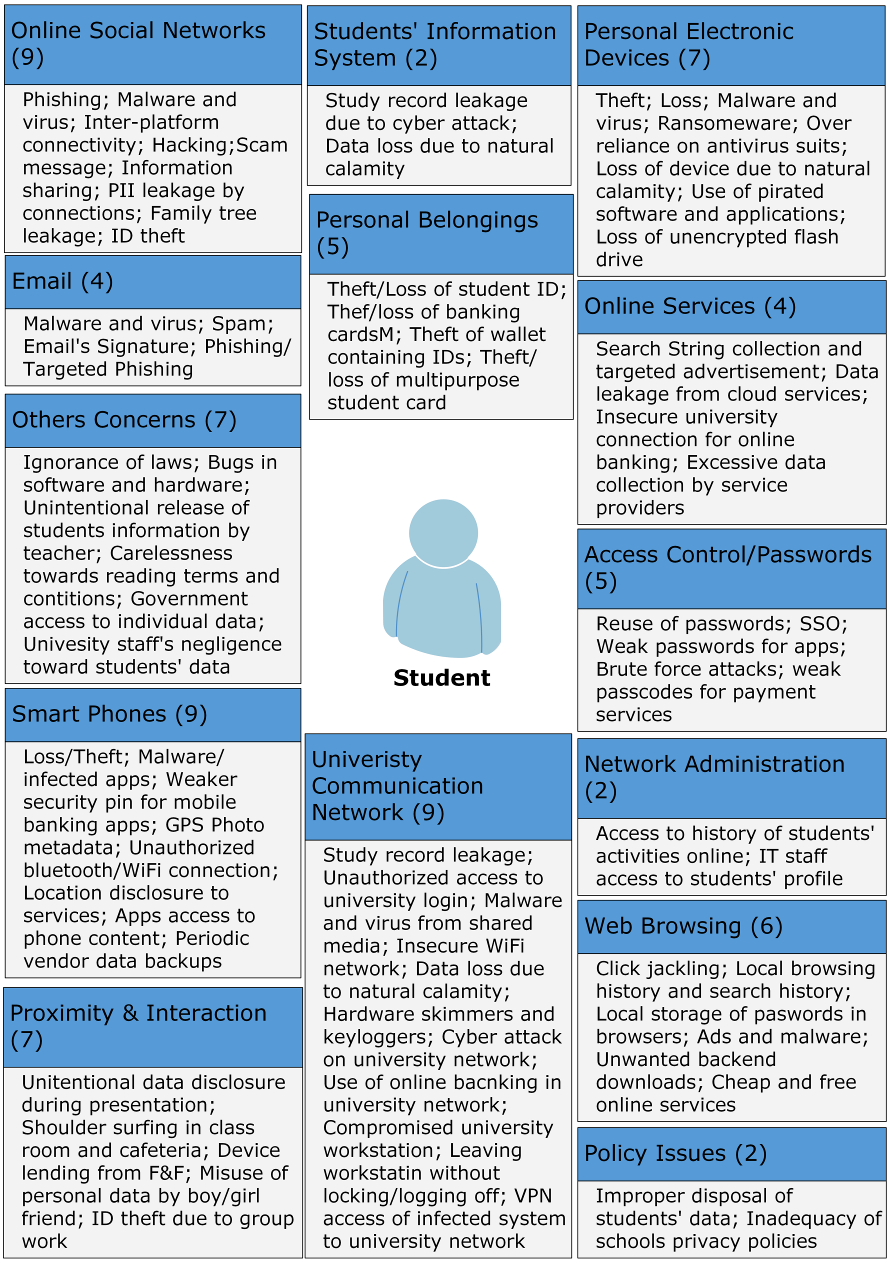
The examination of data collected from the group of students reveals that they mentioned seventy-five different IS&P threats. In this study, the focus was to identify the perceived threats and not to prioritise them. Furthermore, we did not inquire about the consequences of these threats and possible countermeasures against them. Identified threats were then classified using content analysis. Most of the identified threats were related to security and privacy. However, there were a few related to surveillance, and they were not considered for this study. The participants showed their concerns regarding a wide range of threats, from online social networks (OSNs) to the university's communication network and from smartphones to their wallets.

4.4.1 Subjectively Categorized Areas of Concern

Students' perceived information security concerns were grouped into fourteen areas. Each area along with the concerns is shown in **Figure 4.3**. Next is a succinct description of each area and corresponding concerns as mentioned by the students:

1. Personal Belongings. Respondents identified non-electronic items such as the student ID card, banking cards (debit and credit cards) and the wallet as essential items regarding their information security. Nowadays, students have a multipurpose student ID enabling them to access different facilities within the university, such as printing services and the library as well as using it as a payment card in the cafeteria. The theft/loss of such cards can deprive the students of these services, and if fallen in the wrong hands, the information stored in the cards can be misused. The respondents also mentioned that their wallets contain important items that can compromise their privacy if the wallets are fallen into the hands of a malicious party. Losing a banking card can result in financial loss to the students. Therefore, theft/loss of the personal belongings was considered a privacy threat by the students.

2. Proximity/Interaction. The respondents mentioned that they feel their information security at risk while interacting with their peers and class fellows at the university. One respondent suggested that someone peeping onto the laptop's screen can steal his passwords for university login or even for online banking credentials. Other mentioned that a similar peeping at the university's cafeteria could disclose banking card details (cardholder name, card number and the customer verification code (CVC)). Another respondent mentioned someone is looking at laptop screen from the back row in class may know what she is doing or even copying her assignment(s).



Online Social Networks (9)

Phishing; Malware and virus; Inter-platform connectivity; Hacking;Scam message; Information sharing; PII leakage by connections; Family tree leakage; ID theft

Email (4)

Malware and virus; Spam; Email's Signature; Phishing/ Targeted Phishing

Others Concerns (7)

Ignorance of laws; Bugs in software and hardware; Unintentional release of students information by teacher; Carelessness towards reading terms and contitions; Government access to individual data; Univesity staff's negligence toward students' data

Smart Phones (9)

Loss/Theft; Malware/ infected apps; Weaker security pin for mobile banking apps; GPS Photo metadata; Unauthorized bluetooth/WiFi connection; Location disclosure to services; Apps access to phone content; Periodic vendor data backups

Proximity & Interaction (7)

Unitentional data disclosure during presentation; Shoulder surfing in class room and cafeteria; Device lending from F&F; Misuse of personal data by boy/girl friend; ID theft due to group work

Students' Information System (2)

Study record leakage due to cyber attack; Data loss due to natural calamity

Personal Belongings (5)

Theft/Loss of student ID; Thef/loss of banking cardsM; Theft of wallet containing IDs; Theft/ loss of multipurpose student card

Student

Univeristy Communication Network (9)

Study record leakage; Unauthorized access to university login; Malware and virus from shared media; Insecure WiFi network; Data loss due to natural calamity; Hardware skimmers and keyloggers; Cyber attack on university network; Use of online bacnking in university network; Compromised university workstation; Leaving workstatin without locking/logging off; VPN access of infected system to university network

Personal Electronic Devices (7)

Theft; Loss; Malware and virus; Ransomeware; Over reliance on antivirus suits; Loss of device due to natural calamity; Use of pirated software and applications; Loss of unencrypted flash drive

Online Services (4)

Search String collection and targeted advertisement; Data leakage from cloud services; Insecure university connection for online banking; Excessive data collection by service providers

Access Control/Passwords (5)

Reuse of passwords; SSO; Weak passwords for apps; Brute force attacks; weak passcodes for payment services

Network Administration (2)

Access to history of students' activities online; IT staff access to students' profile

Web Browsing (6)

Click jackling; Local browsing history and search history; Local storage of paswords in browsers; Ads and malware; Unwanted backend downloads; Cheap and free online services

Policy Issues (2)

Improper disposal of students' data; Inadequacy of schools privacy policies

Figure 4.3: Students’ Concerns related to their Information Security

[Header contains the title of the functional area followed by concerns mentioned by the students. Semicolons separate the concerns.]

Other concerns included: connecting a laptop to a multimedia projector in a classroom and accidentally revealing their passwords on the big screen. In addition to that, the respondents also mentioned possible threats that could come from connections such as friends and boy/girlfriend. For example, lending their devices (mobile, laptop etc.) to their friends is a potential risk as their friends may explore their devices – accessing SMS messages, emails or even pictures; boy/girlfriend gets to know their passwords and upon breakup, may access their account(s), change password(s) or even blackmail them. One of the female participants considered making a group on a social media platform and working together for class assignments as a potential privacy risk.

3. Smart Phones. Some reports have shown smartphones as one of the most significant information security threat to an organisation [145], [224]. A perusal of the respondents' responses revealed that they were also concerned about threats related to smartphones. The number of concerns related to smartphones was more than concerns identified for any other focus area. Theft, loss, malware and infected apps were among the information security concerns. Furthermore, weak security codes for mobile banking (four digits) were also considered as a security threat. The respondents considered unauthorised Bluetooth or WiFi connections as a security threat. Regarding privacy, location disclosure to apps, GPS photo metadata, an app's access to phone contents and periodic backups by app vendors were also among the concerns.

4. Other Personal Electronic Devices. All the perceived threats (concerns) related to the laptops, computers, mobile phones, tablets and flash drives were put into the category of personal electronic devices (PEDs). The concerns particular to smartphones have already been discussed above. The respondents considered malware and viruses, use of pirated software, over-reliance on anti-virus suits and ransomware as information security threats and noted them as concerns. The loss/theft of any of the devices mentioned above, the theft/loss of an unencrypted flash drive, and device losses due to a natural calamity such as fire, earthquake or an accident were among other identified concerns.

5. Network Administration. The respondents showed their concerns over authorised and unauthorised access to students' profile information, browser's browsing history and activity log on the university network by IT staff. There seemed to be a trade-off between effective network management and students' perceived information security threats.

6. Policy Issues. Respondents of the study also identified policy-related issues that can be possible information security threats for the students; for example, the inadequacy of privacy policies at the university. They also considered the school's information retention policies, wherein students' information (personal and educational) is kept for a certain number of years before disposal, as a potential privacy threat to the students.

7. University Communication Network. The respondents mentioned some concerns related to university communication networks, for example, malware and virus infections from the university's shared storage media, an insecure wireless network, a compromised workstation on the university network, hardware skimmers and keyloggers. Using an online banking service on the university network was considered a potential financial risk. Students log into a university workstation in the library and forgetting to log off was mentioned by several participants as well. Access to the university network via VPN from an infected machine was also perceived as a threat.

8. Students' Information Systems. The respondents mentioned a couple of concerns related to students' information systems. The respondents believed that an attack on the university network could result in leakage of students' records which is a privacy threat to them. Furthermore, any unauthorised access to students' records in the university can expose the students to security and privacy threats. Destruction of devices containing students' information due to natural calamities was another information security concerns.

9. Email. Email is one of the most often tools used for communication these days. It is also used as a medium to phish users' credentials. Like other users, students are prone to a wide range of security threats while using email. The respondents mentioned malware, viruses, spam, phishing/targeted phishing as information security concerns. Nonetheless, unintended use of email signature was considered as a privacy risk by a couple of respondents.

10. Online Social Networks. A previous study on online social networks suggests that the use of OSNs among students is on the rise [145]. The participants in our study mentioned some information security concerns related to online social networks. They cited phishing, malware, viruses, spam messages, hacking and inter-platform connectivity as their concerns. Excessive information sharing by themselves, personally identifiable information (PII) shared by their connections and the leakage of family tree information were among the top concerns mentioned by more than one respondents. One of the participants said that his lack of social media presence makes impersonation easier for a malicious intent entity and since he does not have any social media account, someone can create a fake account and impersonate him.

11. Online Services. According to Kim[144], the use of online services is on the rise amongst students due to online resources such as MOOCs and digital libraries. Students use search engines and cloud services for both learning and recreational purposes. The participants in our study mentioned data leakage from cloud services, search string collection by search engines and targeted advertising, data collection by service providers (websites and web services) and insecure connections while using online banking or user authentication as some of the concerns related to online services.

12. Web Access. Students access the internet for different educational and recreational purposes. Therefore, it was interesting to see what of their concerns are related to the Internet or web. From the data of this study, we found that respondents were concerned with threats related to browsers, malware and unwanted download. The respondents considered the browsing history and the search history saved in the browsers as a threat to their information security and privacy. Furthermore, they also mentioned local storage of passwords (remember my password option) as a perceived IS&P threat. Click-jacking, Ads that install malware and unwanted application downloads were the other concerns mentioned by the participants. They also perceived cheap and free online services as a threat because it leads to potential spamming.

13. Passwords. Passwords are a cost-effective and easily implemented method for authentication yet poor password management practices lead to security issues [225]. Some participants in our study mentioned that poor management of passwords, such as the reuse of a password pose a severe threat to their information security. Among other concerns, the study participants mentioned the use of weak passwords and inherent weakness of passcodes for payment services (mostly four digits), brute force attacks against passwords and single sign-on (SSO) as information security concerns.

14. Others. From the data that we collected from the participants, there were some concerns which could not be put under one of the thirteen categories mentioned earlier. So, we put them into the "others" category. Examples of such concerns were: ignorance of students resulting in possible malicious action that is punishable under certain laws,
carelessness towards reading terms and conditions of the apps and services, government access to a private company's data on an individual, negligence of university staff that results in privacy issues for the students, unintentional release of students' records that are searchable through search engines, threats caused because of bugs in the software and hardware and sharing links to unencrypted files in Dropbox to unintended recipients by mistake.

4.5 Results of Quantitative Study

As described in Section 4.3.4, PCA was employed to identify the underlying factors of the data. The 11-factors solution was found to be a stable solution. Items abbreviations, item loadings and the abbreviation for factor title are shown in **Table 4.4**. For item description consult **Table 4.2.**

23 items were dropped while attaining reliable and stable factors. List of such items is shown in **Table 4.5**.

The 11-factors solution has 2-9 items. We examined each factor and given a title based on the items loaded on the respective factor. Each factor depicted an area where students had shown concerns related to their information security. To assess the reliability of the factors, we calculated Cronbach's alpha for each factor and found all factors to be above an acceptable level (0.70).

Factor 1 (F1) consists of concerns related to online social networks and thus given the title "Online social networks use" [OSN] (α=0,922). Factor 2 (F2) depicts concerns related to lapses by university staff and named "Staff members lapses" [STAFF] (α=0,853). Factor 3 (F3) shows students' lack of awareness towards reading terms & conditions of application and knowing about local cyber laws and termed as "Legal awareness" [LEGAL] (α=0,762). Factor 4 (F4) depicted the concerns related to the university's network and termed as "University networks" [UNET] (α=0,916). Factor 5 (F5) consisted of concerns related to web browsing and emails and named "Web browsing and email" [B&E] (α=0,909). Factor 6 (F6) consists of concerns that may arise due to interaction with family members, friends, classmates or while working with the class fellows and thus termed "Sociality" [SOC] (α=0,862). Factor 7 (F7) consists of concerns that may arise while using smartphones and termed "Smartphone Use" [SPH] (α=0,901). Factor 8 (F8) shows concerns that are related to theft or loss of non-technical items, such as cards and wallets, losing which may result in a threat to information security of the students. This factor was named "Cards and Wallets security" [C&W] (α=0,927). Factor 9 (F9) consists of concerns related to conventional threats such as phishing and brute force attack and, thus, named "Conventional threats" [CTHR] (α=0,817). Factor 10 (F10) related to personal electronic devices (PEDs) and named "PED Use" [PED] (α=0,822). The Factor 11 (F11) consists of concerns that may arise due to service/application providers and named as "Intrusive Service Providers" [SPRV] (α=0,725). (The abbreviations mentioned after each factor title are used in the Figures and Tables and are discussed here for better readability)

S#	CC	F1	F2	F3	F4	F5
		OSN	STAFF	LEGAL	UNET	B&E
1	OSN7	0.78				
2	OSN6	0.78				
3	OSN5	0.76				
4	OSN8	0.74				
5	OSN9	0.63				
6	OC3		0.71			
7	OC6		0.67			
8	OC4			0.66		
9	OC1			0.51		
10	UCN3				0.67	
11	UCN4				0.67	
12	UCN7				0.66	
13	UCN2				0.64	
14	UCN6				0.62	
15	UCN5				0.61	
16	UCN1				0.60	
17	UCN8				0.60	
18	SIS2				0.57	
19	WA3					0.65
20	EM2					0.64
21	EM1					0.63
22	WQ4					0.60
23	WA2					0.59
24	WA5					0.57
25	WA6					0.56

[CC: Concern codes; Factors are denoted by F1 to F6 along with abbreviations of factor titles]

Table 4.4: Factors along with Item Loadings Depicting Information Security Concerns of Students

S#	CC	F6	F7	F8	F9	F10	F11
		SOC	SPH	C&W	CTHR	PED	SPRV
26	PnI6	0.80					
27	PnI5	0.78					
28	PnI3	0.75					
29	PnI2	0.74					
30	PnI7	0.73					
32	SP4		0.75				
33	SP6		0.70				
34	SP5		0.68				
35	SP7		0.62				
36	SP3		0.58				
37	SP8		0.54				
38	PB4			0.86			
39	PB3			0.85			
40	PB2			0.84			
41	PB1			0.77			
42	OSN1				0.78		
43	PW4				0.74		
44	EM4				0.68		
45	OSN3				0.51		
46	PED4					0.71	
47	PED2					0.69	
48	PED3					0.67	
49	OS1						0.76
50	OS3						0.70
51	OS2						0.64

[CC: Concern codes; Factors are denoted by F1 to F6 along with abbreviations of factor titles]

Table 4.4 (continued): Factors along with Item Loadings Depicting Information Security Concerns of Students

S#	Code	Concern
1	WA4	*ClickJacking*
2	PnI4	*Lending devices to Friends*
3	PED1	*Theft/Loss of personal electronic devices (PEDs)*
4	PED5	*Ransomware in PEDs*
5	PED6	*Loss of device due to natural calamity*
6	PED7	*Loss of unencrypted flash drive*
7	SP1	*Theft/Loss of smartphone*
8	SP2	*Malware/Infected Apps in smartphones*
9	PI1	*Improper disposal of students' data*
10	PI2	*Inadequacy of school's privacy policies*
11	NA2	*IT staff access to students' profile data*
12	UCN7	*Compromised university workstation*
13	PW1	*Reuse/one password multiple accounts*
14	PW2	*Single Sign-On*
15	PW3	*Weak passwords*
16	PW5	*Weak passcodes for payment services*
17	OSN2	*Malware and virus in social networks*
18	OSN4	*Scam messages in social networks*
19	OSN5	*Hacking in social networks*
20	OSN6	*Excessive Information Sharing in social networks*
21	NA1	*Access to the history of students' activity online by IT Staff*
22	OC2	*Bugs in software and hardware*
23	OC5	*Government access to individual data*

Table 4.5: List of Security Concerns Removed During the Analysis

4.5.1 Connecting Concerns to Students

To clarify the connection between students and areas of concern, we employed an affinity diagramming technique [226] to group the related areas. An affinity diagram is a tool that is used to organise data (ideas, opinions, issues) into groups based on their natural relationship. Each group is given a header that captures the essential links among the concepts. The titles of all 11 areas were written on sticky notes, and two researchers grouped them based on their natural connections separately.

Once grouping was completed, both researchers shared their grouping, and finally, they come across an affinity diagram consisting of 5 groups covering 11 areas of concern. Each group was given a title and represented one of the day-to-day facets of a student's life. **Figure 4.4** depicts areas of concerns and how they relate to students' everyday life.

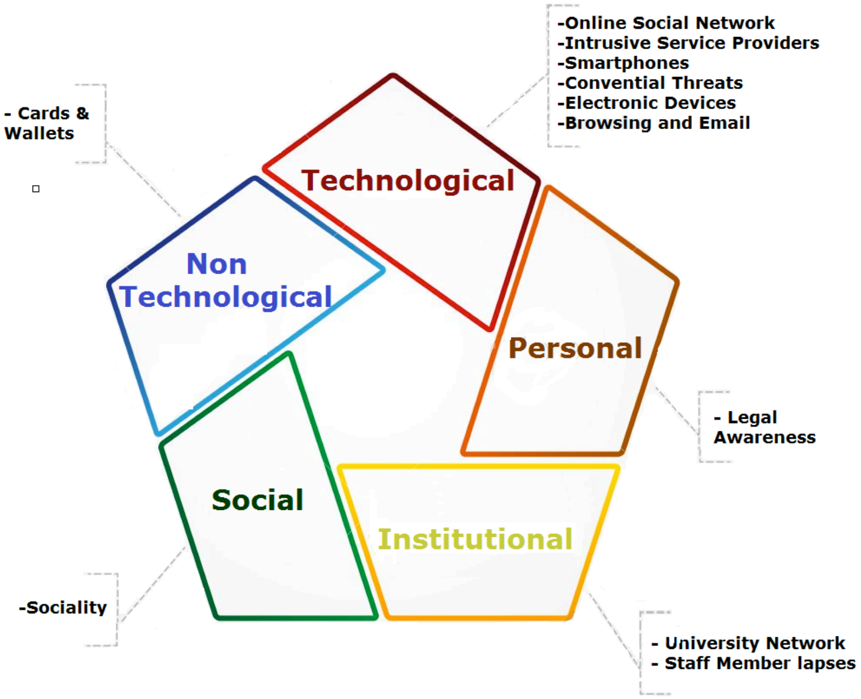


Figure 4.4: Areas of Concerns and Different Aspects of Students' Life

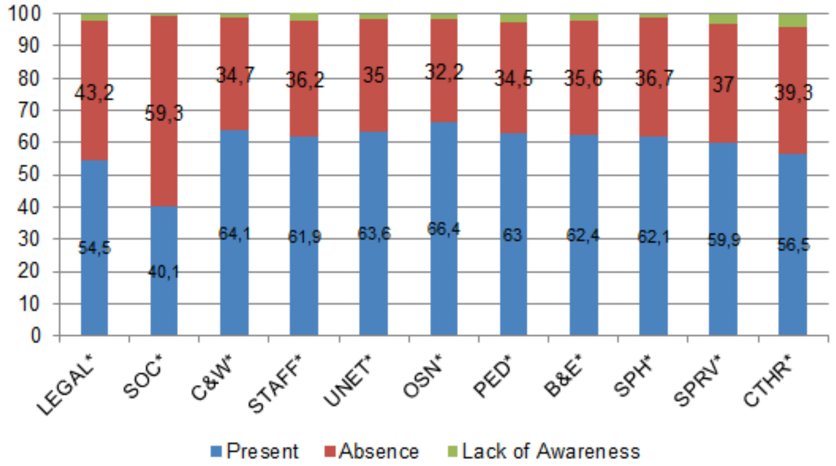
The Personal dimension contained concerns related to awareness of cyber laws (legal awareness). The Social Dimension includes concerns that may arise due to interactions with family, friends and peers at educational institutions (sociality). The Institutional Dimension includes concerns related to educational institutions such as the university network and staff members. Technological Dimension has concerns related to online social networks, smartphones, conventional threats, electronic devices, and online surfing; and non-technological dimension contains concerns about theft or loss of cards and wallets.

The dimensions mentioned above were formulated based on the subjective judgement of the researchers. One may argue that university networks, an area which is part of the institutional dimension can be part of the Technological dimension. Logically, it is correct. However, keeping in mind the day to day life of students, the area was more suited to Institutional dimension rather than the technological dimension.

4.5.2 Prevalence of Concerns

Once areas of concern were identified, we next examined how prevalent are concerns among the students within the identified areas. For this, we divided the area concern score into three groups, 1) Absence of Concern, 2) Presence of Concerns, and 3) Lack of awareness. The 7-point ordinal scale was converted to the nominal scale using the following coding. We encoded "not at all concerned (1)", "low concern (2)", "Slightly concerned (3)" and "Neutral (4)" as absence of concern (0); and "moderately concerned (5)", "very concerned (6)" and "extremely concerned (7)" as presence of concern (1). Moreover, the originally coded "I don't know (0)" was coded as 2. Although there has been quite a debate in the literature on reducing the ordinal scale to a nominal scale among the social scientists, our purpose of examining the prevalence was well served using this technique. This approach was also employed by [220] while quantifying users' beliefs about software updates and putting them into three factors. We, then, calculated the percentage of prevalence of concerns within an area.

Figure 4.5 shows the prevalence of concerns in different areas. Further, we employed chi-square test to test and found that the difference in the prevalence of concerns was significant (depicted by * with area code in the figure) for all the areas ($p<0.05$). In comparison, the highest number of respondents (66%) have concerns related to online social networks (OSN), whereas, the area for which least number of respondents (40%) have concerns was sociality (SOC). Except for SOC, more than half of respondents (at least 54%) have concerns within all the areas.



(p<0.05)

Figure 4.5: Prevalence of Concerns within Areas with significant differences (p<0.05)
[Legal Awareness (LEGAL), Sociality (SOC), Cards and Wallets Security (C&W), Staff Members Lapses (STAFF), University Networks (UNET), Online Social Networks (OSN) Use, Electronic Devices Use (PED), Web Browsing and Email (B&E), Smart Phones Use (SPH), Intrusive Service Providers (SPRV), Conventional Threats (CTHR)].

4.5.3 Level of Concerns

While the prevalence of concerns shows if concerns are present or absent within an area among the students, the level of concern enables us to see how concerns vary among the students. Descriptive of the concern scores within each area was examined to assess the level of concerns. While taking the mean, mode, median and standard deviation, we did not include the responses depicting awareness of concern (the originally coded "I don't know (0)) and considered them missing for this phase. **Table 4.6** shows descriptive for 11 identified areas in descending order of mean scores.

From **Table 4.6**, we can see that the average (mean) concern level for most of the areas was higher than "neutral" (4) and close to "moderately concerned" (5), except for Sociality where mean score was less than 4. The highest level of concern was found related to intrusive behaviour by service providers such as search string collection by search engines, targeted advertisement, excessive data collection by service providers for marketing purpose and data leakage from the cloud services. The lowest level of concerns was related to

Sociality. The concerns within this area were mostly connected to family members, close friends and peers in the classroom and university. Intrusive Service Providers, Cards and Wallets security, Online Social Networks, Smart Phones and Staff Lapses turned out to be the top 5 areas where students have a higher level of concerns.

#	Areas	N	Mean	Median	Mode	SD
1	SPRV	343	5.02	5.33	7	1.48
2	C&W	350	5.01	5.50	7	1.95
3	OSN	349	5.00	5.60	7	1.79
4	SPH	350	4.95	5.17	7	1.70
5	STAFF	347	4.93	5.50	7	1.78
6	PED	345	4.83	5.00	7	1.74
7	UNET	349	4.82	5.00	7	1.60
8	CTHR	339	4.76	5.00	7	1.70
9	LEGAL	346	4.75	5.00	7	1.85
10	B&E	347	4.74	4.86	7	1.62
11	SOC	352	3.82	3.83	1	1.76

Table 4.6: Result of Means, Medians, Modes, Standard Deviations for the level of concerns for different areas *[Intrusive Service Providers (SPRV), Cards and Wallets Security (C&W), Online Social Networks Use (OSN), Smart Phone Use (SPH),Staff Members Lapses (STAFF), Electronic Devices Use (PED), University Networks (UNET), Conventional Threats (CTHR), Legal Awareness (LEGAL), Web Browsing and Email (B&E), Sociality (SOC)]*

4.6 Summary

Existing information security awareness (ISA) studies are either narrowly focused regarding studied areas or merely based on suggestions of security experts. To have "in-depth defence" for higher education institutions a comprehensive ISA approach is required where ISA is assessed holistically, covering all aspects of users' life, and involve end-users' input from the very beginning of the ISA process. This study investigated students' concerns about information security and identified 11 areas. Further, analysis of prevalence suggested that almost half of the students had information security concerns in all the aspects, except for the social expect where only 44% of the students showed concern. The examination of the level of concern provides evidence that the identified areas are existent among students of different gender, age and educational backgrounds. A small percentage of students showed a lack of awareness in areas such as legal awareness, staff members lapses, electronic device use, web browsing and email, intrusive service providers and conventional threats.

The study shows that students perceive to have information security concerns in both online and offline threats. Offline concerns stem from theft and loss of documents containing personal information, as well as from social interaction with classmates and friends. Quite surprisingly some offline security concerns also dealt with family members. While concerns prevailed in all the areas, the top three highest levels of concerns were found to be related to Intrusive service providers, cards and wallets, and online social network use. Gender, age and educational background turned out to influence concerns, whereas, the effect of previous information security training and educational level could not be ascertained.

Apart from the concerns, we also found that most of the students were aware of different types of information security issues about a student. However, in certain areas, a handful of students (about 10%) showed lack of awareness in areas such as legal awareness, staff member lapses, electronic device use, web browsing and email, intrusive service providers and conventional threats.

In the next chapter, we compare security practices of students with that of security expert to ascertain the connection of ISA with the security practices.

Chapter 5

Experts vs Students: Comparing Security Measures and Practices

In the previous chapters, the information security awareness of the students (Chapter 3) and their information security concerns (Chapter 4) have been examined. In this chapter, we compare the security behaviours of students with the security professionals to ascertain if there is a difference between their security behaviours. This chapter relates to the $\boldsymbol{O_3}$ of the thesis.

Like in any other organisation, information security is one of the concerns for the educational institutions [176]. The availability of vast amounts of computing power and open access has attracted the attention of malicious entities towards higher educational institutions (HEIs) [146]. Students make a large portion of users in HEIs and are attractive candidates for online threats [185]. The Internet is an integral part of university students' daily life. They use computers and internet for a variety of purposes [190] such as accessing email, completing course assignments, accessing course materials, using online course management systems, retrieving grades, purchasing books and other stuff, paying fees and conducting other transactions that involve their personal information. Students leave a significant amount of their sensitive information online. This dependency can expose students to different information security threats that can not only compromise their information security but also of the others around them, such as family members, peers and even their educational institutions. For example, an unaware student can download malware into their home computer by clicking on the ad which may collect critical information from all those who use the computer. Moreover, "bring your own device" (BYOD) policies makes students responsible for the security of the device. However, an incompetent device owner can compromise the security of the educational institutions.

Despite this fact that students use the university network and follow the IT policies of an HEI, they are not as bound as an HEI employee [186]. Students are the future workforce who upon completion of their degrees will serve in different organisations in different roles. Some of them will be future security experts while others will take roles of ordinary employees. It is of paramount importance that students be trained so that they exhibit secure behaviour online. Information security education, which includes security training and awareness programs, can be used to make computer and internet users security conscious [66]. Such training should introduce students to different security concepts as well as offer advice which is realistic as well as practical.

Researchers suggest a multi-layered "defence in depth" approach, where users are required to perform more than one security behaviour [189]. Security experts recommend a variety of security measures and advice to the end-users for their safety online [227]. Most of the advice was given in the area of system security, account security, email security and web security. However, a recent study showed that non-home users differ in security practices from what security experts do or recommend [228]. However, there is no comparative study where security practices of students are compared with that of security experts.

Building upon the work of Ion et al. [228], this study aims at identifying the security measures taken by HEI students and compare their security practices with that of experts. In this regard, data of students' security practices were collected using an online questionnaire, whereas data related to experts' security practices were taken from [228]. For analysis, we ran Pearson's Chi-square with post hoc test, and effect size (Cramer's *V)* was calculated to examine the differences. Ion et al. only looked at Chi-square tests without a post hoc test.

The rest of the chapter is organised as follows: Section 5.2 explains the methodology used in this study, followed by the results presented in Section 5.3. The conclusions are given in section 5.4.

5.1 Methodology for Comparative Study

5.1.1 Research Questions

This study aims to 1) identify which security measures students consider most important towards protecting their security online, and 2) compare their security practices with that of security experts. For this purpose, the following research questions were used:

> ***RQ1: What are the top security measures taken by the students for their security online?***
>
> ***RQ2: Are there any differences between the security practices of students and security experts?***

In this study students are university-level students, enrolled in a Bachelor or Master level program, and the security experts are people "having at least five years of experience working or studying computer security" [228].

5.1.2 Instrument

The instrument consisted of questions adapted from the previous work [228]. The questionnaire was divided into two parts.

The first part asked participants about their gender, age, nationality, educational background, degree major and current level of education. *Gender* was asked on dichotomous scale (Male/Female). The participants were asked to enter their *age* in number of years (continuous). Like gender, *nationality* was also asked using a dichotomous scale (Finnish/International). Participants were asked to mention their *educational discipline* by selecting one of the following: Business/Economics, Education, Humanities, Information Technology/Computer Science, Other Engineering, Law, Medicine, Natural Sciences including Mathematics, Social Sciences and Others. For current *educational level* participants could select from one of the followings: Bachelor, Masters, Doctoral/Licentiate, Other. In addition to above participants were also asked to mention their degree major in form of free text. This information was necessary for comparison (detail in section 5.1.4).

Part II of the questionnaire consisted of one open-ended question about security measures and 13 questions (multiple-choice) about security practices of the participants. At the beginning of Part II, the participants were asked to state, "the three most important things they do to protect their information security online". The participants had free space to give their answer. Out of 13 questions, two were about system security, three each for web security and email security, and five for access control (password creation and management). The statements of these questions are given in **Table 5.1**, whereas, their measurement scales are described in the result section.

5.1.3 Data Collection

Using Google forms, an online questionnaire consisting of 20 items was distributed as a pre-course survey amongst 400 university students in four cybersecurity-focused courses (two each at bachelor and master levels) at a Finnish university. The courses were mandatory for IT and information security major students while students from other disciplines could voluntarily take these courses. No financial benefit was given to the survey participants.

Security Measures [Open ended]

Q1. What are the 3 most important things you do to protect your security online?

Practices

System Security [MCQ]

Q2. How soon after you discover that a new version of the operating system (OS) is available, do you (or somebody else managing your computer) install it?

Q3. Do you use anti-virus software on that computer?

Web Security [MCQ]

Q4. Do you look at the URL bar to verify that you are visiting the website you intended to?

Q5. Do you check if the website you're visiting uses HTTPS?

Q6. Do you visit websites you have not heard of before?

Email Security [MCQ]

Q7. Do you open emails you receive from people or companies you don't know?

Q8. Do you click on links that people or companies you don't know send you?

Q9. Do you enter your password to the website, to which you have reached by clicking a link in an email?

Access Security

Q10. Do you use two-factor authentication (e.g., 2-Step Verification) for at least one of your online accounts? *[MCQ]*

Q11. How do you keep track of your passwords for your online accounts? *[MCQ Grid]*

i) Remember them
ii) Write them down on paper
iii) Have my password manager (e.g., 1Password, LastPass) remember them
iv) Use the same password on multiple accounts

Table 5.1: Questionnaire (Part II) with items description

Data related to experts was collected from an already published study where security practices of experts and non-experts were compared [228]. Additional information and the necessary permission were received from the first author of the mentioned study.

5.1.4 Data Analysis

Most of the respondents were male students (73% of 354). Ages of respondents ranged from 18 to 53 (Mean:23.64, SD:5.46), with 70% in the 18-24 age range, 25% in the 25-34 age range, and 5% in the 35-53 age range. 90% of the students were Finnish whereas 10% were international students. 75% of the students were from IT, including computer engineering, discipline, whereas the rest were from disciplines such as humanities, natural sciences and social sciences. 23% of the students were enrolled in a Master's degree program in cybersecurity (termed as semi-experts), whereas the rest had different majors at bachelor level degrees (termed as novices). Explanation of grouping into semi-experts and novices is given in section 5.5.

Among the experts (N=231), 4% were female. Age ranged from 18 to over 65, with 30% in the 25-34 age range, 32% in the 35-44 age range, 18% in the 45-54 age range. Almost half of the experts were American (47%) and the rest from other countries. 73% of the experts held a Bachelor's degree or higher. 69% of the experts were working in the industry, 15% in academia, 13% were self-employed, 11% in government and 7% in corporate research labs [228].

The respondents were asked to state the three most important things they do to protect their digital security. The responses from the students were analysed by two researchers using the quantification technique [229]. The security measures were identified as mentioned from what was mentioned by the respondents. The security measures were coded and compared between two coders for reliability. Percentage (to a nearest whole number) of each category of practices questions (Q2 to Q11) was calculated. Pearson's Chi-square was used for comparison of practices. p-values were corrected for multiple testing using the Holm-Bonferroni method. The effect size was calculated using Cramer's V. Further, to identify the source of difference between the students' and the experts' practises, we divided the students into two groups: Semi-experts and novices. Semi-experts were the students having formal cybersecurity-related education and novices were the students who were without formal education in cybersecurity or a related field. A post hoc test was conducted to pinpoint the differences. The following interpretation of the effect size was used: Weak (0-0.20), Moderate (0.20-030), Strong (0.30-0.50) [230]. The acceptable range of effect size is 0.20 to 0.50.

5.2 Results

5.2.1 Top Security Measures

The content analysis of the responses to the open-ended question (Table 5.1: Q1) revealed that altogether as many as 64 things are done by students for their online security. There were ten practices which were followed by at least 5% of the students including limiting the digital footprint/avoiding the sharing of personal information(PI) (36%), using strong passwords (33%), using anti-virus/anti-spyware software (29%), being critical and suspicious/using common sense (27%), updating Operating System (16%), using unique passwords (15%), avoiding the clicking Ads and links (7%), using incognito mode (6%), not using specific apps & services (5%) and avoiding suspicious/harmful sites (5%).

On the other hand, the security measures adopted by at least 5% of the experts were: updating the system (35%), use unique passwords (25%), using a two-factor authentication (20%), using strong passwords (19%), using a password manager (12%), avoiding the sharing of PI (10%), checking for HTTPS (10%), using verified software (8%), using Anti-virus/anti-spyware software (29%), using Linux (6%) and being critical and suspicious (5%).

A comparison of experts' and students' security measures mentioned by at least 5% of each group is given in **Figure 5.1**.

5.2.2 Practices related to System Security

Updating the operating system and using anti-virus/anti-spy software were among the top 5 security measures taken by the students for their online security (Figure 5.2). Both measures are related to system security. To further investigate students' behaviour towards system security we asked two questions (Q2 and Q3 in Figure 5.1).

Figure 5.2a and 5.3b show the comparison of responses from students and security experts related to system security along with Chi-square statistics.

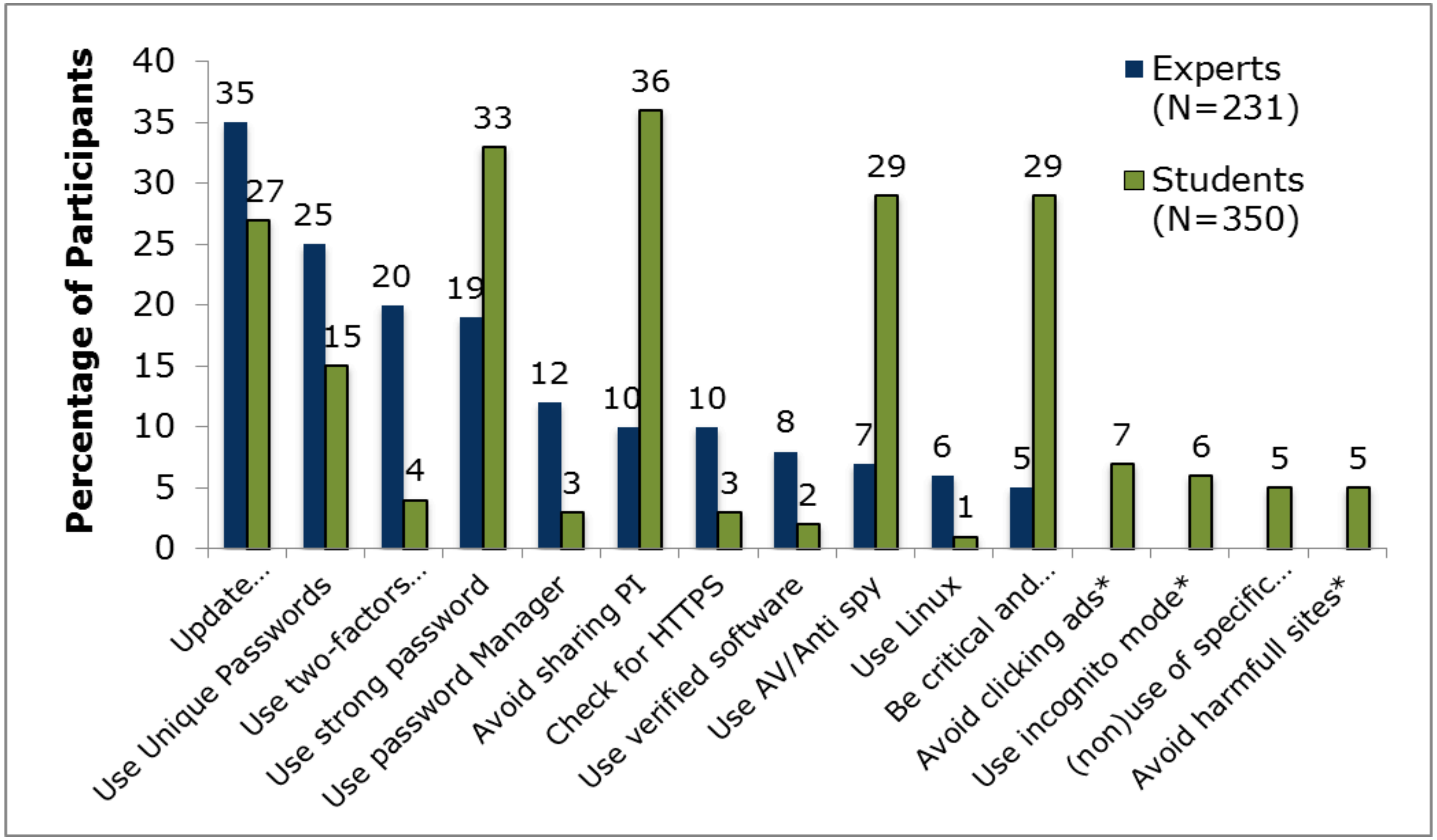


Figure 5.1: Top Security Measures mentioned by at least 5% of Students and Security Experts
[data for security experts was not available]*

The Chi-square statistics showed that students and experts differ significantly in how soon after do they install updates become available, they install them (effect: strong), and in the number of anti-virus software users (effect: moderate). Fewer students than experts (46% vs 64%) immediately update the operating system when becoming available. More students than experts (16% vs 4%) never install an operating system update. In the case of anti-virus software, more students than experts (85% vs 63%) use such software for their security.

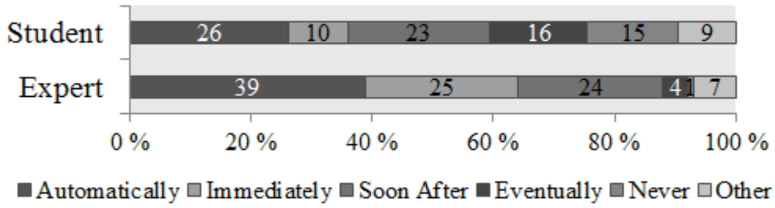


Figure 5.2a: Comparison of Security Practices -How soon after do you install updates? *($X^2(5)=73.59$, $p<0.05$, $V=0.36$)*

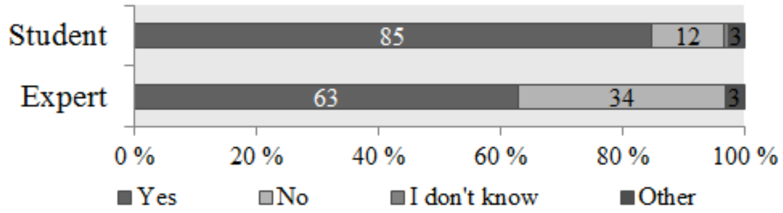
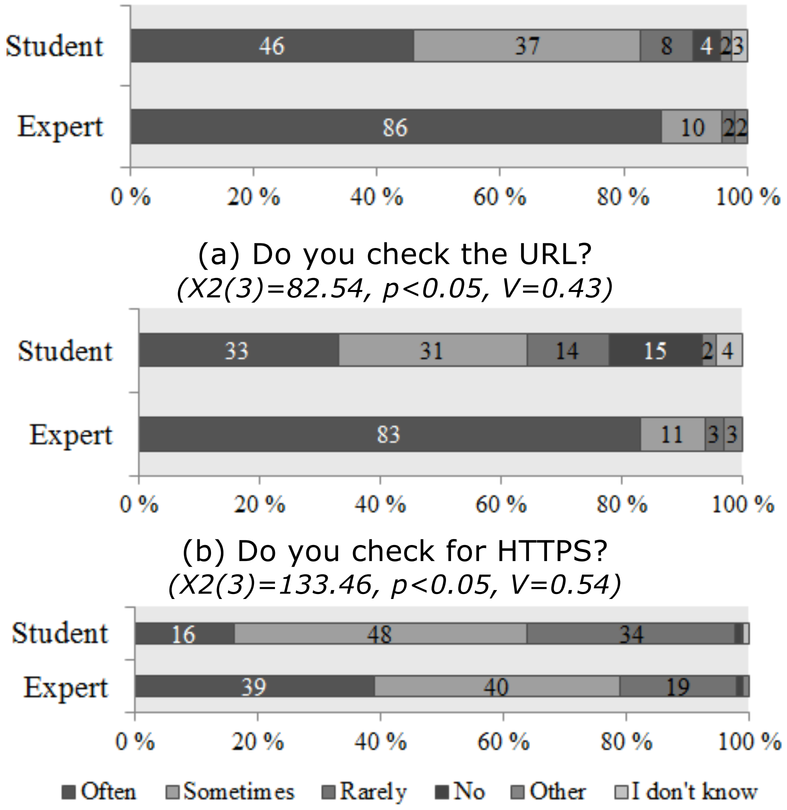


Figure 5.2b: Comparison of Security Practices -Do you use Anti-virus software?
($X^2(3)=32.53$, $p<0.05$, $V=0.27$)

5.2.3 Practices related to Web Browsing

Web browsing is one of the primary functions that an internet user performs. It is typically done for a collection of information through known and unknown information spaces (like websites and forums). However, due to the increased number of hoax and phishing sites, web browsing poses threats such as identity theft, losing credentials, financial frauds and loss of data. Students regarded the limiting of their digital footprint or avoiding the sharing of their personal information (36%) and being critical and using common sense (29%) as the top 3 measures they take for their security online. However, other measures such as verifying the URL (1%), checking for HTTPS (3%), and visiting only known/trusted sites (3%) were not quoted among the most repeated measures for security online.

To further examine students' security practices related to web browsing, we asked three questions (Q4 to Q6 in **Table 5.1**). The responses were taken on six categories; "often", "sometimes", "rarely", "No", "I don't know" and "others". **Figure 5.3** shows the students' and experts' responses for each of the questions mentioned above, along with Chi-square statistics.



(a) Do you check the URL?
(X2(3)=82.54, p<0.05, V=0.43)

(b) Do you check for HTTPS?
(X2(3)=133.46, p<0.05, V=0.54)

(c) Do you visit new websites?
(X2(3)=32.53, p<0.05, V=0.27)

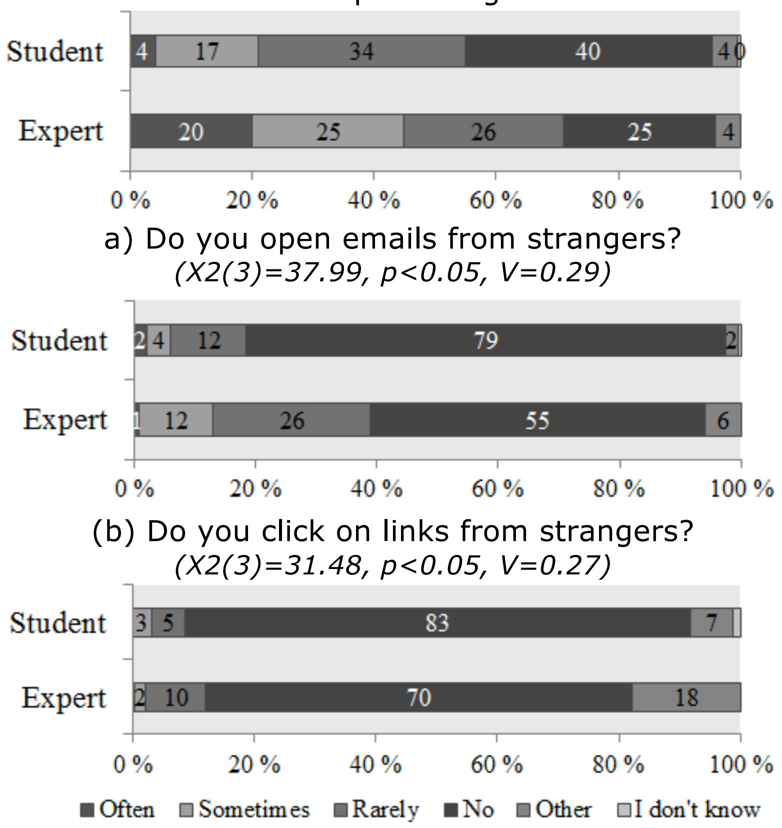
Figure 5.3: Comparison of Security Practices related to Web Browsing, between Students and Experts

Chi-square statistics show that students and experts have significant differences in checking the URL (effect: strong), checking for HTTPS (effect: strong) and whether they visit new websites (effect: moderate). Fewer students than experts often check the URL (46% vs 86%), check for HTTPS (33% vs 83%), and visit new websites (16% vs 39%).

5.2.4 Practices related to Email Security

Figure 5.1 shows that none of the security measures taken by at least 5% of the students was related to email security. Although passwords are linked to emails, we will discuss them separately in the next section.

We inquired about security practices related to email security using three questions (Q7 to Q9). The students had options to select from the following six categories; “often”, “sometimes”, “rarely”, “No”, “I don’t know” and “others”. **Figure 5.4** shows a result in percentage.



a) Do you open emails from strangers?

(X2(3)=37.99, p<0.05, V=0.29)

(b) Do you click on links from strangers?

(X2(3)=31.48, p<0.05, V=0.27)

(c) Do you enter a password to the website…?

(X2(3)=6.19, p=0.10, V=0.13)

Figure 5.4: Comparison of Security Practices related to Email Security, between Students and Experts

Chi-square values show that students and experts differ in their practices related to (Q7): opening emails (effect: moderate) and (Q8): clicking on links from the strangers ((effect: moderate)). However, no significant difference was found in the case of Q9 (p=0.10). Fewer students than experts at least sometimes open emails from strangers (21% vs 45%), whereas, more students than experts never click on the links received in emails from the strangers (79% vs 55%).

5.2.5 Practices related to Access Control

Using strong passwords was one of the top 3 security measures taken by the students (**Figure 5.1**). On the other hand, experts prescribe measures such as the use of unique passwords, two-factor authentication and a password manager as the top security measures [227], [228]. To examine behaviour related to account access (passwords), we asked five questions from the students and compared their responses with those of the security experts.

One of the questions (Q10) was about the use of two-factor authentication for which students were to reply by selecting one option from the following: "yes", "no", "I don't know" and "other". Other four questions (item i to iv of Q11) were measured on a grid format question having the following options: "For ALL of my accounts", "For MOST of my accounts", "For SOME of my accounts", and "For NONE of my accounts".

Students' responses for each category of Q10 and Q11, as a percentage along with a comparison to the experts' responses are shown in **Figure 5.5(a-e)**. Chi-square statistics with effect size are also provided in all cases. The comparison of student and expert responses showed significant differences in all five cases with effect size ranging from moderate to strong (p<0.05).

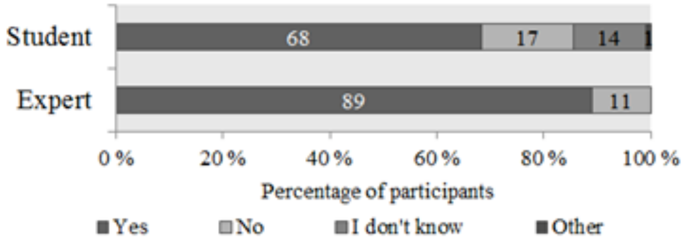


Figure 5.5a: Comparison of Password Management Practices - Do you use two-factor authentication?

(X2(2)=41.20, p<0.05, V=0.30)

There were fewer students than experts (68% vs 89% in Figure 5.5a) use two-factor authentication, whereas, 14% of the students did not know about two-factor authentication. More students than experts (80% vs34%) remember passwords for most of their accounts (Figure 5.5b)

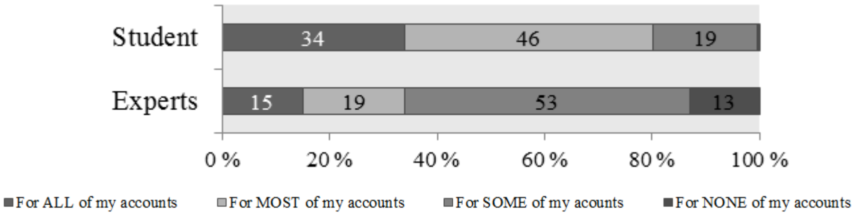


Figure 5.5b: Comparison of Password Management Practices - Do you remember passwords?
(X2(2)=104.48, p<0.05, V=0.48)

More students than experts (38% vs 20%) write down at least some of their passwords on paper (Figure 5.5c). Fewer students than experts (22% vs 74%) use a password manager (Figure 5.5d), and more students than experts (81% vs 45%) use same passwords for at least some of their accounts (Figure 5.5e).

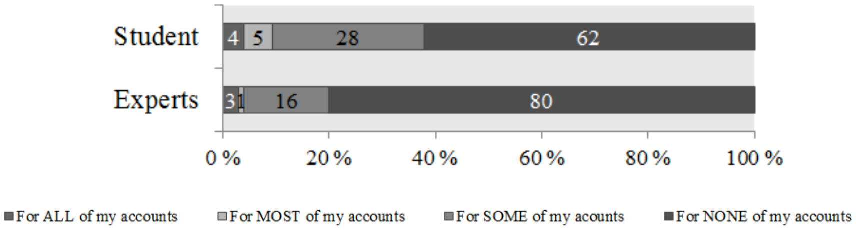


Figure 5.5c: Comparison of Password Management Practices - Do you write your passwords on paper?)
(X2(2)=20.82, p<0.05, V=0.21)

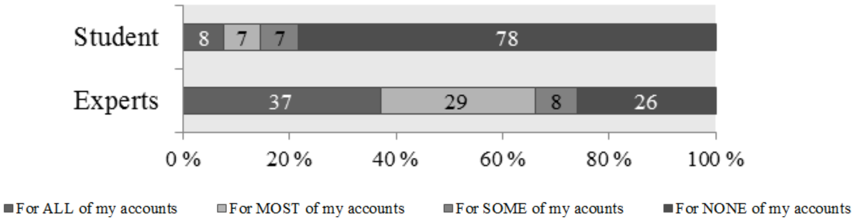


Figure 5.5d: Comparison of Password Management Practices - Do you use a password manager?
(X2(2)=133.10, p<0.05, V=0.54)

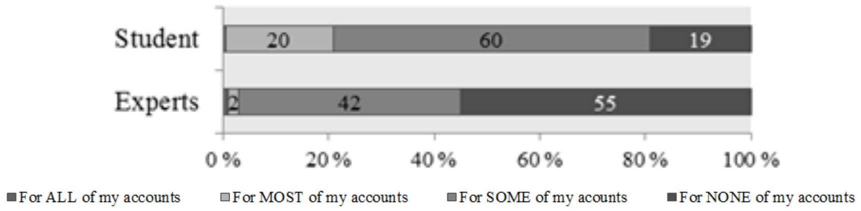


Figure 5.5e: Comparison of Password Management Practices - Do you use same password for multiple accounts? *(X2(2)=80.96, p<0.05, V=0.42)*

5.2.6 Comparing Experts, Semi-Experts and Novices

Since we had two types of students in our sample, semi-experts and novices, we ran a 3xY (where Y represents the number of categories against given practices) Chi-square test to identify the different student group (from the experts).

We also conducted a post hoc analysis with a *p-value* corrected for Holm-Bonferroni adjustments, to identify the exact origin of difference(s). The results are shown in **Table 5.2.** The first column tells the practice under consideration (description in Table 5.1). X2 is Chi-square statistics; *df* is a degree of freedom, V is Cramer V for effect size. Sig. (significance) The column shows if there is a significant difference in practices of semi-experts and novices with experts. Post hoc findings show the exact origin of the difference between each student group and experts. The last column describes if a difference of practice could result in security risk for the students.

5.3 Discussion and Summary

Students employ a variety of security measures for their security and privacy. However, not all the measures are foolproof. Security experts recommend several security measures for the security and privacy of internet users. Using an online survey, we identified the security measures and practices of 350 university students and compared the practices with those of security experts. The data for security experts were collected from previous research [228].

	X^2	*df*	*v*	Sig *	Difference with Experts	Important Findings	Risk
System Security							
Q2	80.92	8	0.29	Yes	Only Novices	**More novices than experts** (20% vs 1%) **never** install updates. **Fewer novices than experts** (9% vs 35%) do not install updates **immediately.**	**Yes**
Q3	82.89	3	0.30	Yes	Only Novices	**Few novices than experts** (11% vs 35%) do not use antivirus software	**No**
Web Security							
Q4	85.42	6	0.31	Yes	Both Semi-experts and Novices	**Fewer novices than experts** (47% vs 88%) **often** check URL. **More novices than experts** either **rarely** or **never** (15%cs 2%) verify the URL. Similarly, **more novices than experts sometimes** (38% vs 10%) check the URL. **Fewer semi-experts than experts** (50% vs 88%) **often** check URL.	**Yes**
Q5	138.42	6	0.40	Yes	Only Novices	**Fewer novices than experts** (29% vs 86%) **often** check the HTTPS. **More novices than experts** check HTTPS: 1) either **never** or **rarely** (36% vs 3%), and (2) **sometimes** (34% vs 11%).	**Yes**
Q6	35.19	6	0.20	Yes	Both Semi-experts and Novices	**Fewer novices than experts** (18% vs 40%) **often** visit new websites. **More semi-experts than experts** (42% vs 19%) **rarely** visit new websites.	**No**

Table 5.2: Comparison of security practices of semi-experts and novices with security experts

	X^2	*df*	*v*	Sig. *	Difference with Experts	Important Findings	Risk
Email Security							
Q7	35.79	6	0.20	Yes	Only Novices	**Fewer novices than experts** (5% vs 21%) **often** open emails from unknown senders	**No**
Q8	33.84	6	0.20	Yes	Only Novices	**More novices than experts** (83% vs 56%) **never** click on a link in the emails received from the unknown parties. **Fewer novices than experts sometimes** (3% vs 13%) and **rarely** (11% vs 28%) do the above-mentioned action.	**No**
Q9	6.06	6	0.09	No	None		
Access Control							
Q10	556.5	4	0.25	Yes	Only Novices	**More novices than experts** (16% vs 6%) do not know about two-factor authentication.	**May be**
Q11 (i)	108.2	6	0.34	Yes	Only Novices	**More novices than experts** remember passwords for **all** (35% vs 15%) and **most** (49% vs 19%) of their accounts. **Fewer novices than experts** (16% vs 53%) remember passwords for **some** of their accounts	**Yes**
Q11 (ii)	26.10	6	0.17	Yes	Only Novices	**More novices than experts** (31% vs 16%) write passwords on paper for **some** of their accounts.	**Yes**
Q11 (iii)	135.9	6	0.39	Yes	Both Semi-experts and Novices	**Fewer novices than experts** use password managers for at least **most** of their accounts (14% vs 66%) **Majority of semi-experts than experts** as compared to experts (80% vs 26%) do not use password managers.	**May be**
Q11 (iv)	82.89	6	0.30	Yes	Only Novices	**More novices than experts** (22% vs 2%) use the same password for multiple accounts. **Fewer novices than experts** (18% vs 55%) use unique passwords	**Yes**

Table 5.2(continued): Comparison of security practices of semi-experts and novices with security experts

Chi-square test was conducted to compare the security practices of the students and the experts. The comparison showed that security measures taken by students differ from the measures taken by security experts.

Top three measures taken by students were avoiding of sharing of personal information/limiting the digital footprint, using a strong password and using of anti-virus/anti-malware software, whereas, as the top 3 measures experts update their system more often, use unique passwords and use two-factor authentications. Moreover, the comparison of students' security practices with security experts showed a significant difference. For example, fewer students than security experts immediately update their operating systems, check the URL, check for HTTPS, visit new websites, open emails and click on the links in the emails, use two-factor authentication and a password manager. Also, more students than experts use anti-virus software, remember passwords for at least most of their account, write down passwords and use the same password for at least some of their accounts.

A post hoc analysis showed that semi-expert (students having cybersecurity as their degree major) behave similarly to experts and even when they behave differently, their behaviour may not jeopardise their security. On the other hand, novices (students without a formal security education) not only differ from experts more often in their practices but also, their deviating behaviour can put their system security, web security and password security at risk.

While we have examined the differences in practices between students and experts thoroughly, this study is not without limitations. IT students dominated our student sample. A bigger sample of non-IT students might have caused more deviant behaviours to surface. The items used to measure practices were, in fact, pieces of security advice from experts. In the future, we will examine the connection between perceived goodness (perceived effectiveness and likelihood to follow) and the practices. It will help us identify the advice which students consider useful are willing to follow. It will also be interesting to assess the role of the source of advice towards the perceived goodness. We may have to investigate other disciplines, too, to identify the factors affecting perceptions of the advice receiver. In this study, we have considered only three areas for measuring and comparing security practices.

Chapter 6

The Relationship between Security Awareness and Security Behaviour: An Explanatory Study

This chapter presents explanatory study explaining the relationship of information security awareness and security behaviour using IMB Model. This chapter relates to $\boldsymbol{O_4}$.

The pervasiveness of the Internet has provided a variety of technical and social benefits to us. The numbers of internet users are multiplying with each passing day. It is estimated that 54% of the world population will be using the internet by the end of 2018 (Internetworldofstats.com). While at one end, the internet has brought a variety of benefits to us, we are also exposed to the dark side of the Internet due to different information security threats [4]. To mitigate these security threats, organisations implement not only technical measures [9]but also, non-technical or educational measures, such as information security policies and security education, training and awareness programs (also known as SETA programs) [10]–[12], [57].

Like other businesses, information security has been an issue for educational institutions in the past [176]. And today it has become one the of biggest challenges for the educational institutions especially higher educational institutions (HEIs) [29], [147], [231]. The importance of HEIs has increased manifold for a nation in the era of the knowledge-based economy. Educational institutions, especially higher education institutions (HEIs), serve large populations of students but also maintain the technological infrastructures to support the learning and research activities. HEIs often manage large computer centres which collect private information of students and staff, and crucial research information [146]. If compromised, these resources can be misused by malicious entities. For example, leveraging denial of service attack, identify theft of staff and students, and selling products information for financial gains.

Unlike other organisations, HEIs have two distinct groups of human resource, employees and students, both of which are subject to information security policies. As users are regarded as the weakest link in the information security [5], measures should be taken to improve the security behaviour of both staff and students in HEIs. In this regard, it is important to understand users’ (both staff and student) security behaviours in the HEI context. Some theory-driven approaches have been used in information security research to explore which factors influence security behaviour to identify ways in which the security behaviours of users may be improved. To date, researchers have utilised as many as 54 theories in the context of information security [98], [102], [104]. Some researchers have studied the relationship between security behaviour and information security awareness using theories such as Protection Motivation Theory (PMT) and Theory of Planned Behaviour (TPB) [34]–[36].

This study presented in this chapter seeks to contribute to the existing body of research in two ways. First, a new theory-based model, Information-Motivation-Behavioural Skills (IMB) Model [118], [119] has been tested to study security behaviour of the users in the context of HEIs. Second, we empirically validate the relationship between security awareness and security behaviour.

The IMB Model posits that information and motivation are the key prerequisites towards a given behaviour. These prerequisites connect to behaviour through the behavioural skills of the person. This model has not been tested empirically in the context of information and cybersecurity to date except for Crossler and Belanger's work [127] who used IMB model to propose a conceptual framework highlighting the mobile privacy-security knowledge gap model.

To achieve our objectives, that is checking the applicability of IMB model in the context of information security behaviours and empirically validating relationship of information security awareness and security behaviour; data was collected from a set of Finnish University students in 2017 using an online survey. The data was then analysed in SmartPLS 3.0 using structural equational modelling.

The rest of the chapter is structured as follow: Section 6.2 provides the theoretical background and an overview of different theories used in a security context, followed by a description of the IMB Model, the research model constructed on the basis of this model and other theory components. Section 6.3 outlines the methodology and data analysis. Section 6.4 describes the results, followed by the discussion in Section 6.5.

6.1. Theories Related to Security Behaviour

Security researchers have been using different theories borrowed from other disciplines to study security behaviour. However, four behavioural theories have been used predominantly. These are Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), Technology Acceptance

Model (TAM), and General Deterrence Theory (GDT). Among these theories(and models) PMT [128], [232] and TPB [107] has been used predominating in the security literature[98], [102], [104], [129], [233].

TPB was proposed in 1991. According to TPB [107], intention predicts behaviour and intention are predicted by three motivational factors: Attitude, subjective norms, and perceived behavioural control. Here attitude is a person's feelings to perform certain behaviour, for example, using two-factor authentication to improve password security. Subjective norms depict a person's perception of what is expected of him and her environment about a certain behaviour (e.g., such as information sharing on social media). Perceived behavioural control refers to the extent to which a person can engage in a behaviour, given the circumstances and consists of two components, self-efficacy and perceived controllability. Self-efficacy captures the degree to which one feels capable of performing the behaviour. It captures the extent to which control is within reach of the person (e.g., securing a system from viruses). Perceived controllability may reflect the extent to which a person feels they have the available resources to perform a given behaviour, such as keeping a system clear of malware.

PMT theory was proposed originally in 1975 [232]. The purpose was to understand how fear appeals influence behaviour. This theory is composed of two parts: Threat appraisal and coping appraisal. Threat Appraisal determines the adaptability of coping behaviour regarding perceived severity, vulnerability and maladaptive rewards. Here perceived severity refers to the degree that a threat will generate negative consequences (e.g., the result of somebody accessing an unlocked space to steal data). Perceived vulnerability reflects the perceived likelihood that one will fall a victim of a threat if no action is taken (e.g., perceived risk of becoming a victim of a phishing attack when clicking on a link in an email). Maladaptive rewards represent intrinsic and extrinsic motivation (more precisely the benefits) that one perceives to have by evading the desired behaviour (e.g., evading a system update to avoid having to learn to use a new user interface). Coping appraisal in PMT captures the person's sense of how efficient, manageable and costly their risk-reducing behaviour is given the situation the person faces [128]. Coping appraisal in PMT theory consists of three components: Self-efficacy, response efficacy, response costs. Self-efficacy is similarly constructed and defined as in TPB. Response efficacy is a belief that a certain action will reduce the threat, for example, verifying URL may prevent a phishing attack. Response costs refer to the perceived cost associated with a coping action (e.g., learning to use password manager is time-consuming).

As we saw in the above discussion the two most preferred theories (TPB and PMT) in information security behaviours research deal with motivation and beliefs. TPB has constructs such as attitude and subjective norms that measure the motivation, whereas, the constructs such as perceived behavioural control in TPB and constructs related to threat appraisal and coping appraisal are related to an individual's beliefs. According to Meichenbaum & Turk [115], the behaviour is operated by four independent factors: Knowledge and Skills, beliefs, motivation and action. If any of these factors are deficient, the behaviour may not as it is required. Here *knowledge and skills* refer to the necessary information of the problems, solutions, importance and self-regulatory behaviour. *Beliefs* are related to threat appraisal (perceived severity, perceived vulnerability) and coping appraisal (self-efficacy, response cost, response efficacy). *Motivation* is value and reinforcement as well as internal attribution of success. Motivation can be intrinsic or personal or extrinsic or social. And, lastly, the *actions* which are stimulated by cues, and steered by information recall. Existing theories and models used in security behaviours literature take some of these factors into account. For example, TPB takes attitude, subjective norms and self-efficacy into account which covers motivation and beliefs. PMT is based on beliefs (coping appraisal and threat appraisal) whereas TAM and GDT also deal with the belief system. So, we need a model or theory that takes more than just motivations and beliefs into consideration.

6.2 The IMB Model

The IMB Model was proposed in 1992 to predict health-related behaviours [118]. Initially, the model was used to predict adherence behaviour related to AIDS (HIV) through information, motivation and behavioural skills. This model is built upon the earlier work to construct a simple model to guide thinking in complex health behaviours. Since then it has been applied to predict positive changes related to health behaviours (other than AIDS) [120]–[122], [234], drug use [235], cancer screening [134], [236] voting behaviours [123] and recycling behaviours [124]. Although few of the security researchers have proposed the use of IMB model in the context of security and privacy, it has not yet been tested empirically [125]–[127], [130], not especially in the context of HEIs information security.

The IMB Model consists of three variables: information, motivation and behavioural skills. According to the IMB model, behavioural skills directly predict the behaviour, and behavioural skill is influenced by both information and motivation of the individual. There is an association between information and motivation as well. **Figure 6.1** shows the complete IMB model.

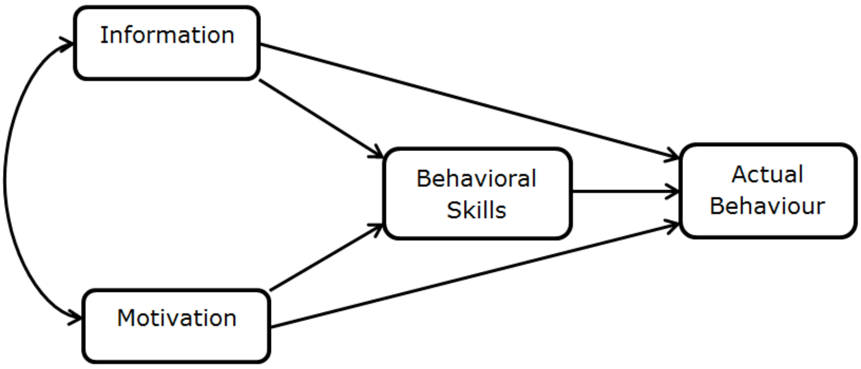


Figure 6.1: Information-Motivation-Behavioural Skills (IMB) Model [118]

Information is a prerequisite to a correct and consistent enactment of given behaviour [118], [119], [122]. An individual can hold accurate information (that will help in the performance of the desired behaviour) and inaccurate information (that may impede the desired behaviour). Information in the context of information security and privacy may, for example, refer to awareness of the risks related to their use of various devices such as mobile phones [127]. In the information security domain, the concept of information has been referred to as awareness. The assumption, therefore, is that if a person is aware of information security (risks and threats), he or she will have a more positive attitude and intention to comply with security policies and behave securely. Threat perception plays an important role in the selection of appropriate security measures [16]. Crossler & Bélanger [127] suggest that IMB Model provides an important link between information (awareness of threats/risk), and development of knowledge and skills to behave securely. Therefore, we propose that information in the context of security behaviour may be assessed using threat awareness, as this would imply individuals have information (more or less) about threats in the security landscape.

The second predictor of behaviour is motivation which is considered a critical component for engaging in and maintaining required behaviours [128]–[130]. Motivation includes both personal and social motivation and is influenced by different sources. One can engage in the desired behaviour if the person is highly motivated and have a positive attitude towards the desired behaviour. Motivation may also increase or decrease based on the individual's perceptions of social support toward specific behaviour. For example, individuals may be more motivated to follow security advice if close others support and encourage this behaviour. Social support can be captured through social norms, which is the extent to which individuals follow shared behavioural guidance, which implies their belief as to which security behaviour others will support. Therefore, we propose that personal motivation to engage in secure behaviour is captured by the security attitude of individuals (as these would be strongly correlated), while social motivation may be captured by subjective norms to guide the behaviour in the context of security.

Behavioural skills are proposed as a mediator variable between the two predictors and security behaviour. An individual needs to possess the necessary skills to engage in certain behaviours, in both the health and security domain [128]–[130]. Skills include objective skills and self-efficacy to deal with challenges. Lack of technical know-how (knowledge) limits an individual's ability to perform securely [237]. "Knowing something and wanting to protect oneself is not sufficient if the individuals do not have the necessary skills to perform the required behaviour". Self-efficacy has been extensively studied in the context of information security as it is one of the main constructs in TPB and PMT around which most of information security research revolves [5], [232]. There are mixed views on how behavioural skills can be measured. While most of the others resort to self-efficacy to operationalise behavioural skills construct [120], [132], few others have used perceived difficulty[135], [234], and assessment of knowledge related to skills [124][127] to operationalise the same construct. Considering the fact that we were conducting a survey, measuring objective information security skills was not possible, we resort to measuring behavioural skills as a combination of self-efficacy and subjective assessment of security measures knowledge. "Measures knowledge" was measured by measuring respondents' familiarity with security measures. According to Jeske & Schaik [239], "awareness may not necessarily indicate more than a fleeting degree of knowledge", whereas familiarity can measure a deeper understanding driven by experience in a given context. Therefore, we propose that security knowledge in the context of security behaviour may be assessed using familiarity with security measures.

Finally, like TPB, the dependent variable in the IMB Model is actual behaviour (rather than behavioural intention).

In line with the above discussion, we propose the following modified research model (**Figure 6.2**), to examine the applicability of IMB Model in the context of information security.

6.3. Methodology for Explanatory Study

6.3.1. Sample and Procedure

Participants were recruited from a large, public university in the Southwest of Finland. All 376 prospective participants were enrolled in a blended learning course related to cybersecurity at the time of the study. Of these, 169 students took the two-part survey (response rate = 45%).

The first part of the survey included most IMB Model constructs (information, motivation and behavioural skills). The second part included an assessment of security behaviour. After removing incomplete responses, 159 responses were retained. While no financial or academic benefits were provided, participants were entered a prize draw for movie tickets.

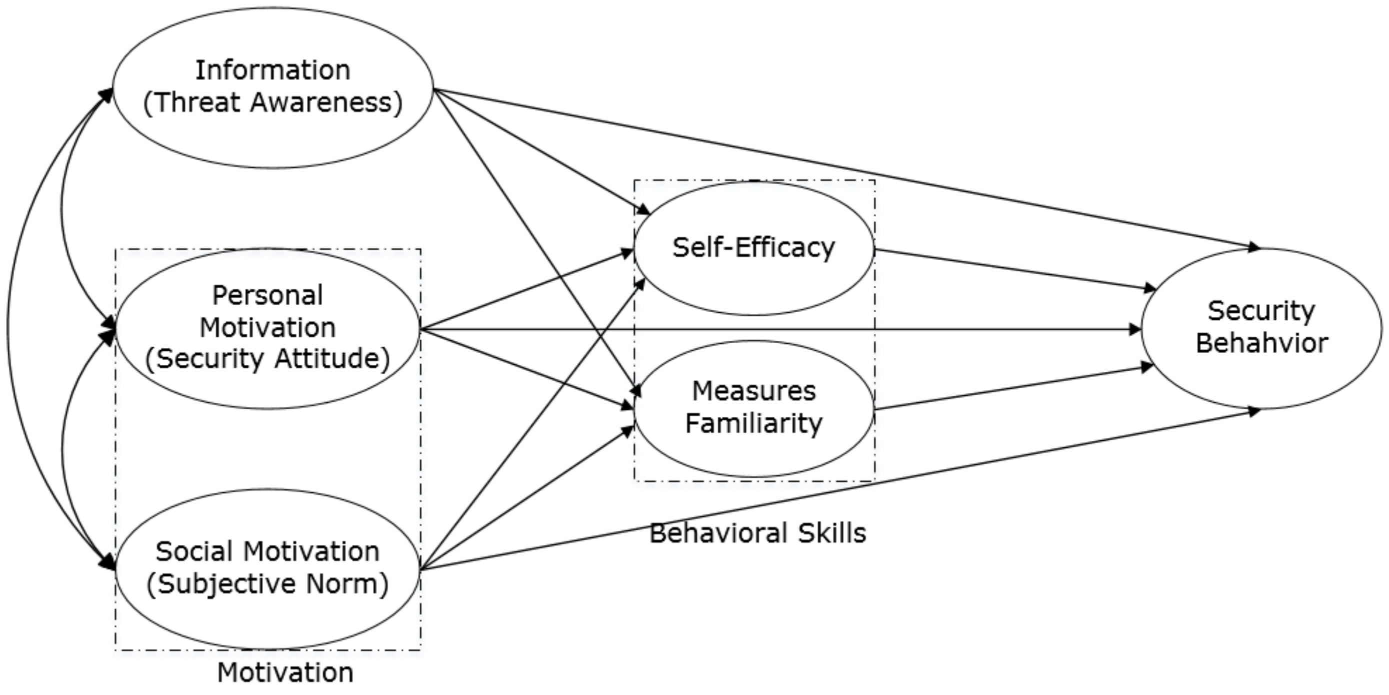


Figure 6.2: Research Model for the Study based on IMB Model

6.3.2. Measures

The questionnaire contained demographic queries (gender, age, education, discipline, work and Internet experience). Several existing measures were utilised to assess the constructs chosen for information, motivation, behavioural skills and security behaviour. **Table 6.1** shows the IMB model constructs, constructs in our research model and the operational definition of each construct, followed by the description of the constructs. For description of constructs consult **Appendix B**.

IMB Model Constructs	Constructs in Research Model	Operational Definition
Information	Threat Awareness	The extent to which a participant is aware of security threats.
Motivation	Personal Motivation (Attitude)	The extent to which a participant feels about security.
	Social Motivation (Subjective Norms)	The extent to which participant feels that others motivate for engaging in a secure behaviour.
Behavioural Skills	Self-efficacy	The extent to which participant believes he/she is equipped to deal with security threats and exhibit secure behaviour.
	Measures Familiarity	The extent to which a participant is familiar with security measures.
Behaviour	Security behaviour	The extent to which participant follows prescribed security advice.

Table 6.1: Constructs and operational definitions

Information was measured in terms of "threat awareness". To measure threat awareness, 20 security threats (taken from our work presented in Chapter 4 [238] and work of Jeske & van Schaik [239]) were presented to respondents to rate their awareness on 5-point scale ranged from 1=very poor to 5=excellent. The list consisted of the following threats: Trojan, botnet, identity theft, cookies, virtual stalking, internet surveillance, theft/loss of devices, malware, shoulder-surfing, rogueware, theft/loss of cards and wallets, spyware, information leakage in social network, social engineering, data harvesting (applications), keylogger, virus, phishing, zero-day attack and email harvesting.

Motivation was measured in terms of "personal motivation" (attitude towards security), and "social motivation" (subjective norms) [118], [119]. The attitude was measured using four items, adapted from [240]. Subjective norms was measured using three items adapted from [172], [240]. Both constructs were measured on a 7-point scale (1=strongly disagree to 7=strongly agree).

Behavioural skills were measured in term of "self-efficacy" and security measures knowledge (measures knowledge). Self-efficacy was measured using six items (adapted from [172], [241]). The measurement scale was like the one used for measuring motivation. To assess "measures familiarity", top 20 security measures prescribed by the security experts (taken from [227]) were presented to the respondents who rated their familiarity on a 5-point scale (1=not at all familiar to 5=extremely familiar). To make sure that respondents do not confuse familiarity with awareness, an explanation [239], differentiating awareness and familiarity, was presented to the respondents before introducing them to the security measures.

Security behaviour was self-reported security behaviour of participants was measured with the help of self-developed scale consisting of 12 items. Each item represents advice given by the security expert. The items were taken from [228]. Given the fact that we were trying to measure behaviour through self-reported items, we adopted a scale that measures the frequency of an action (1=never, 2=rarely, 3=sometimes, 4=often, 5=always) and not (dis)agreement (strongly disagree to agree strongly). Egelman and Peer [45] used the same measurement scale for developing security behaviour intention scale (SeBIS).

6.3.3. Data Analysis

Data analysis was carried out in two phases. In the first phase, a measurement model was tested whereas, in the 2nd phase, a structural model was tested. For this purpose, we used partial least squares structural equation modelling (PLS-SEM, Smart PLS 3.2). This technique is estimating complex models when the sample size is small, and data is non-normally distributed [242]–[244].

Measurement model testing includes checking for construct reliability and validity. Our model consisted of constructs which can be divided into two types: reflective and formative [245]. Reflective constructs consist of items that show a common cause where cause flows from constructs to items, whereas, formative constructs are a composite measure summarising a common variation through a set of items. In the case of the formative construct, the causal relationship flows from items to the construct (for further differences refer to [246]). According to Chin [246], in the formative construct, removal of a single item can affect the construct negatively. It is very important to decide a type of construct failing to which may result in findings which are not valid. Jarvis, MacKenzie, and Podsakoff [247] provide a set of guidelines which are helpful in deciding the type of construct. They suggest that researchers may decide type based upon the direction of causality, interchangeability of items, the covariance of items and the nomological view of the items. The direction of causality refers to the direction of a causal relationship between items and construct (like explained above); interchangeability of items means if items have similar content, if so then the construct is reflective otherwise its formative; reflective items co-vary with each other, whereas, formative items do not co-vary; lastly, reflective items have a single nomological view where all indicators refer to the same idea and have same consequences, whereas, formative items may not single nomological view and may have different consequences. Based on the above guideline, the construct of information (threat awareness, measures familiarity) and security behaviour was treated as formative, while the remaining constructs were treated as reflective constructs. (Using a combination of formative and reflective constructs in one model is evident in different fields of research, for example, technology adoption [248] and knowledge management [249].

The quality of formative constructs was measured by assessing collinearity diagnosis and significance of formative items. In this regards, guidelines of [242] were followed. As per guidelines, first, the variance inflation factor (VIF) for formative items be assessed and should be between 0.2 and 5. Secondly, the significance of formative items is tested with the help of significance of outer weights. In case, the outer weights are not significant, outer loadings of formative items are checked. The items, having outer-loadings greater than equal to 0.5, are retained, even if the outer weights are insignificant.

For the formative items having outer-loadings less than 5, the significance of outer-loading is checked. If the outer loadings are not significant for the items (having loading <0.5), such formative items are dropped from further analysis. The measurement statistics (VIF, outer-weight, outer-loadings and corresponding significance (*p*) are shown in **Table 6.2**.

In our data, the VIF values for "measures familiarity" and "security behaviour" were between 0.20 and 3.0, which was within the suggested threshold. However, two items of "threat awareness" had VIF higher than 5.0 (TA3=6.41 and TA5=7.20). Removing of TA5 from the model brings VIF for TA3 to 3.38, which was acceptable as per guidelines [242]. TA5 was removed from further analysis. The VIF for the three formative constructs ranged from 1.24 to 3.82, which were smaller than the threshold of 5. Next to assess the significance of the formative items, the complete bootstrapping procedure with 5000 sub-samples, no sign changes at significance level 0.05 (p<0.05) was run (Step 2 in **Table 6.2**).

Construct / Items	**Step 1**	**Step 2**					
	VIF	**Weights**	**p**	**Sig**	**Loadings**	**p**	**Sig**
Threat Awareness (M=3.38, SD=0.64)							
TA1	2.42	0.283	0.183	NS	0.585	<0.01	**
TA2	2.54	-0.038	0.871	NS	0.552	<0.01	**
TA3[2]	*6.82*						
TA4	2.92	-0.275	0.282	NS	0.548	0.002	*
TA5[2]	*7.20*						
TA6	2.71	-0.043	0.847	NS	0.553	<0.01	**
TA7	2.48	-0.046	0.810	NS	0.590	<0.01	**
TA8	2.75	0.335	0.144	NS	0.692	<0.01	**
TA9	1.58	-0.003	0.986	NS	0.508	<0.01	**
TA10	2.39	0.248	0.317	NS	0.651	<0.01	**
TA11	1.63	-0.015	0.934	NS	0.378	0.016	*
TA12	2.19	0.170	0.372	NS	0.500	<0.01	**
TA13	2.00	0.075	0.674	NS	0.509	0.001	**
TA14	2.49	0.216	0.259	NS	0.691	<0.01	**
TA15	1.80	-0.013	0.946	NS	0.491	0.002	**
TA16	1.74	0.449	0.007	**	0.702	<0.01	**
TA17	1.82	0.144	0.580	NS	0.486	0.004	**
TA18[2]	*2.79*	-0.389	0.053	*NS*	0.198	0.148	*NS*
TA19	2.82	0.107	0.622	NS	0.291	0.042	*
TA20	2.08	-0.090	0.653	NS	0.423	0.004	**

*Note. M = Mean, SD = Standard Deviation, VIF = Variance inflation factor, t = t-test values, sig. = significance, NS = non-significant; * p≤0.05, ** p<0.01;*
[1] Initially VIF was 6.41, [2] Removed from further analysis

Table 6.2: Measurement statistics for formative constructs

Construct	Step 1	Step 2					
/ Items	VIF	Weights	p	Sig	Loadings	p	Sig
Measures Familiarity (M=4.15, SD=0.59)							
MF1	2.359	0.146	0.416	NS	0.492	0.001	**
MF2	2.262	-0.094	0.675	NS	0.492	0.001	**
MF3	2.194	0.052	0.815	NS	0.462	0.001	**
MF4	2.041	0.105	0.607	NS	0.564	0.000	**
MF5	2.779	0.018	0.927	NS	0.437	0.004	**
MF6	1.963	0.089	0.579	NS	0.534	<0.01	**
MF7	2.703	0.453	0.015	*	0.778	<0.01	**
MF8	2.413	-0.001	0.997	NS	0.504	<0.01	**
MF9	1.700	0.042	0.795	NS	0.444	0.002	**
MF10	2.302	0.060	0.756	NS	0.470	0.005	**
MF11[2]	1.738	-0.150	0.349	*NS*	0.176	0.334	*NS*
MF12	1.863	-0.049	0.777	NS	0.425	0.004	**
MF13	1.927	0.053	0.770	NS	0.389	0.008	*
MF14	1.892	0.029	0.870	NS	0.395	0.006	**
MF15	2.493	0.462	0.014	*	0.826	<0.01	**
MF16	2.913	-0.096	0.673	NS	0.638	<0.01	**
MF17	1.922	0.029	0.877	NS	0.381	0.023	*
MF18	2.306	-0.159	0.440	NS	0.575	<0.01	**
MF19	2.057	-0.004	0.984	NS	0.515	<0.01	**
MF20	1.487	0.330	0.014	*	0.645	<0.01	**
Security Behaviour (M=3.38, SD=0.47)							
SB1[1]	*1.214*	-0.103	0.448	*NS*	-0.059	0.733	*NS*
SB2	2.131	0.150	0.491	NS	0.430	0.005	**
SB3	1.366	0.182	0.218	NS	0.561	<0.01	**
SB4	1.230	-0.024	0.853	NS	0.330	0.035	*
SB5	2.098	0.079	0.679	NS	0.440	0.002	**
SB6	1.296	0.121	0.382	NS	0.387	0.007	**
SB7	1.240	0.521	<0.01	**	0.761	<0.01	**
SB8	1.247	0.245	0.159	NS	0.530	0.001	**
SB9	1.326	0.270	0.091	NS	0.619	<0.01	**
SB10	1.141	0.028	0.835	NS	0.285	0.037	*
SB11	1.257	0.113	0.423	NS	0.372	0.006	*
SB12[1]	*1.333*	*0.030*	*0.861*	*NS*	*0.358*	*0.063*	*NS*

Note. M = Mean, SD = Standard Deviation, VIF = Variance inflation factor,
t = t-test values, sig. = significance, NS = non-significant;
** p<0.05, ** p<0.01*
[1]Removed from further analysis

Table 6.2(continued): Measurement Statistics for Formative Constructs

In total four items could not fulfil significance criteria: TA18 had an insignificant outer-weight (p=0.053), and outer-loading less than 0.5 (0.198) and insignificant (p=0.14). MF11 had an insignificant outer-weight (p=0.349), and outer-loading less than 0.5 (-0.059) and insignificant (p=0.733). SB1 had an insignificant outer-weight (p=0.448), and outer-loading less than 0.5 (-0.059) and insignificant (p=0.733). SB12 had an insignificant outer-weight (p=0.861), and outer-loading less than 0.5(0.358) and insignificant (p=0.063).

In this way, five items were dropped from the measurement model, one due to high VIF and four, due to insignificant outer weights and loadings.

The quality of reflective constructs was assessed in terms of constructs' reliability (internal consistency and items reliability) and validity (convergent and discriminant validity) for which guidelines suggested by [242], [250], [251] are used. The threshold values for different measures are shown in **Table 6.3**.

Quality Measure	Criterion	Threshold with reference
Reliability	Internal consistency	Cronbach's alpha > 0.70 [250] OR CR > 0.708 (0.60-0.70 for exploratory reasons) [242]
	Items reliability	Item Loadings > 0.70.[1]
Validity	Convergent validity	AVE > 0.50 [242]
	Discriminant validity	Heterotrait-Monotrait Ratio ($HTMT_{0.85}$) [251]

Note. CR = Composite Reliability, AVE=Average Variance Explained.

[1] *0.40-0.70 are acceptable if removal of items does not improve AVE* [242]

Table 6.3: Threshold Values for the Reflective Measurement Model

The reliability of the constructs was measured through internal consistency and item's reliability, whereas, the validity of the constructs was measured through convergent and discriminant validity. The results of reliability and validity assessment for reflective constructs (attitude, subjective norms and self-efficacy) are shown in **Table 6.4**.

Traditionally, Cronbach's alpha (*α*) has been used as a measure of internal consistency. However, some researchers consider composite reliability (CR) a more suitable measure of reliability in PLS than Cronbach alpha [252]. Therefore, as suggested by [242], we have reported both *α* and CR. Both *α* and CR for three reflective constructs were higher than the suggested threshold (consult **Table 6.3**).

Construct / Items	Mean	SD	Item Loadings	CR	α	AVE
Personal Motivation (Attitude)	5.15	0.78		0.87	0.78	0.70
ATT1			0.88			
ATT2			0.73			
ATT3[1]			*0.60*			
ATT4			0.88			
Social Motivation (Subjective Norms)	3.50	1.35		0.91	0.82	0.84
SN1			0.87			
SN2[1]			*0.58*			
SN3			0.96			
Behavioural Skills (Self-Efficacy)	4.90	0.92		0.85	0.74	0.65
SE1			0.83			
SE2[1]			*0.32*			
SE3			0.78			
SE4[1]			*0.51*			
SE5[1]			*0.47*			
SE6			0.80			

Note. M = Mean, SD = Standard Deviation, Loadings = Indicator loadings, CR = Composite Reliability, α = Cronbach's alpha, AVE = Average Variance Explained.

[1] excluded from further analysis due to loadings <0.70

Table 6.4: Measurement Statistics of Reflective Construct Scales

Item reliability determines the rate of the variance of an item that comes from the latent constructs and is assessed with the help of indicator loadings. All the items having loadings above 0.70 were retained. In sample, five items had item loading less than 0.70: ATT3 (0.60), SN2 (0.58), SE2 (0.32), SE4 (0.50) and SE5 (0.47). These items were removed from further analysis. The remaining items having loadings (from 0.73 to 0.96) were retained. In the final model, both personal motivation and self-efficacy were measured with the help of three, whereas, social motivation was measured using two items.

Convergent validity of the reflective constructs is also proved as AVE for all three reflective constructs was above the recommended value of 0.50. Discriminant validity (DV) is used to describe the extent to which constructs differ from others. Heterotrait-Monotrait (HTMT) Ratio [251] is considered as a more appropriate criterion for assessing DV as compared to Fornell-Larcker criterion [253] and checking cross-loading criterion [242]. **Table 6.5** shows, the HTMT ratio for the constructs. The HTMT ratio is below 0.85 for all the constructs, giving evidence of discriminant validity.

Once the measurement model is tested, the structural model is tested. For this purpose, we examine the standardised path coefficients (*β*), the coefficient of determination (*R^2)*, effect size (*$f^{2)}$*, and significance is tested with the help of *t-value* and *P-V*alue. Detail of structural model testing is given in results.

	Construct	1	2	3
1	Attitude			
2	Self-Efficacy	0.41		
3	Subjective Norms	0.11	0.17	

Table 6.5: $\text{HTMT}_{0.85}$ Ratio Confirming Discriminant Validity of the Constructs

6.4. Results

6.4.1. Sample Characteristics

About 65% of the participants were male. The average age of the participants was 24 years (ranging from 18 to 63 years with SD = 6.94). Most of the respondents were bachelor level students (77%), while the rest were from a Master degree or above. Among the bachelor level students, 45% were the 1st year, 15% were 2nd year, 6% were 3rd year, and 11% were 4th year students. About 69% of the participants were from computer science and information technology disciplines, followed by 23% from the natural sciences, whereas, the rest belonged to other disciplines. Also, 41% of the participants had full or part-time working experience. Their average working experience was 4.29 years. The internet experience (in years) of participants range from 2 to 27 years, with an average of 14 years (SD=4.10).

6.4.2. Validation of Structural Model

The standardised path coefficients *(β)*, the coefficient of determination (R^2) and significance ($p < .05$) of the individual paths in the estimated path analysis are shown in **Figure 6.3**.

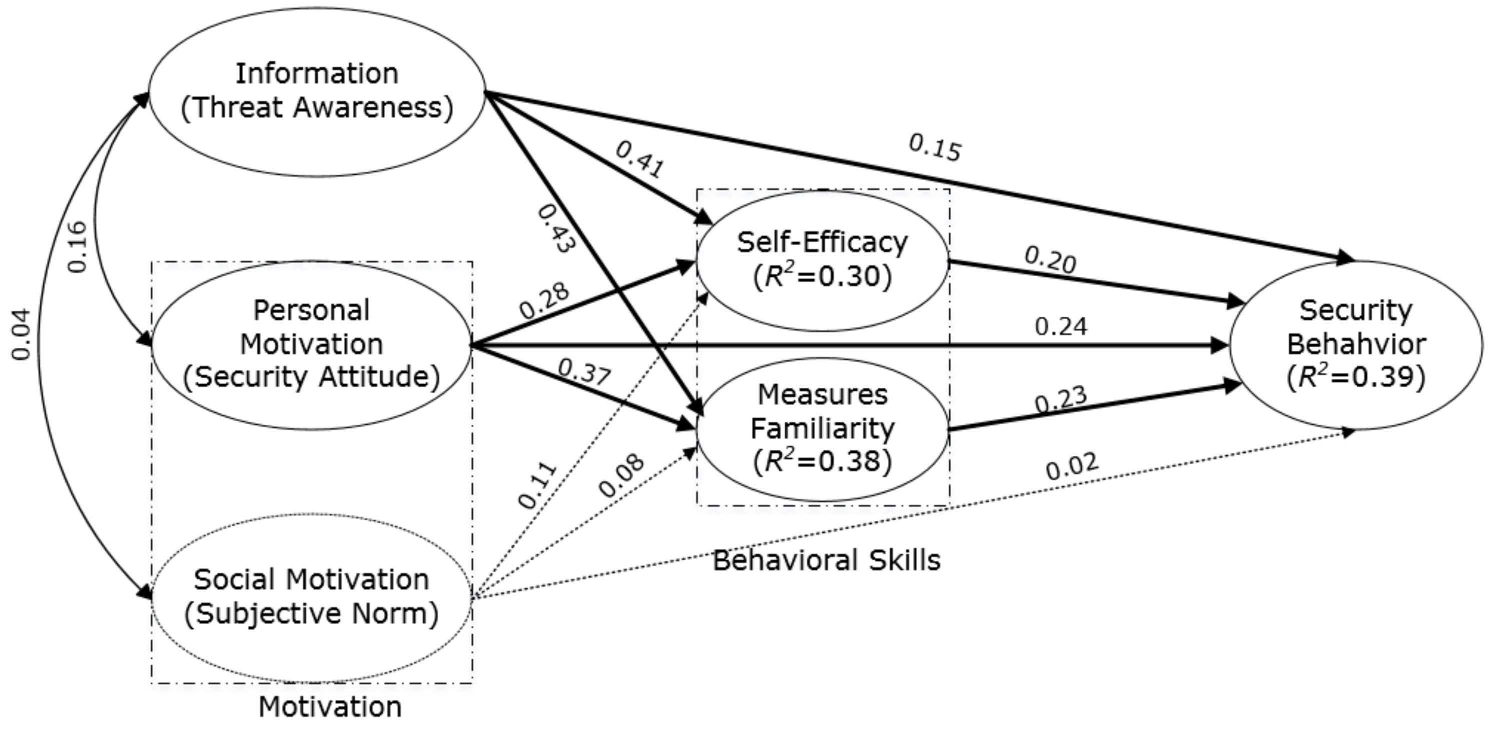


Figure 6.3: IMB model constructs with path coefficients and determination coefficients. Dark arrows show a significant relationship whereas dotted shows insignificant relationship. Double arrows show correlation

We also checked the collinearity of the structural model with the help of predictor construct's tolerance (VIF) and found to be between 1.00 and 1.69. As per [172], [242], VIF coefficient between 0.2 and 5 shows lack of collinearity in the structural model.

As shown in **Figure 6.3**, there were significant direct paths to security behaviour from personal motivation (β=0.24, p=0.005), self-efficacy (β=0.20, p=0.009), and measures familiarity (β=0.23, p=0.02). There were indirect effects of information and personal motivation on security behaviour through self-efficacy (β=0.41, p<0.01; β=0.28, p<0.01) as well as through measures familiarity (β=0.43, p<0.01; β=0.37, p<0.01). Social motivation did not have any direct or indirect significant path to security behaviour. Moreover, information significantly correlates with only personal motivation (r=0.155, p<0.05) and not with social motivation (r=0.04, p>0.05).

For detail statistics on the structural model and correlation consult **Table 6.6** and **Table 6.7**. **Table 6.7** shows that information and motivation (personal and social) correlate with one and other.

Path[1]	**VIF**	***β***	***R^2***	***Adj.R^2***	***t***	***p***	**Sig.**	***f^2***
TA→SE	1.02	0.41			3.313	<0.01	Y	0.23
ATT→SE	1.02	0,28			4.003	<0.01	Y	0.11
SN→SE	1.00	0,11	0.30	0.29	1.691	0.091	N	0.02
TA→MF	1.02	0,43			5.099	<0.01	Y	0.29
ATT→MF	1.03	0,37			3.861	<0.01	Y	0.21
SN→MF	1.00	0,08	0.38	0.37	0.803	0.422	N	0.01
TA→SB	1.47	0,15			1.404	0.160	N	0.02
ATT→SB	1.30	0,24			2.614	0.005	Y	0.08
SN→SB	1.03	0,02			0.326	0.744	N	0.01
MF→SB	1.69	0,23			2.281	0.023	Y	0.05
SE→SB	1.50	0,20	0.39	0.37	2.514	0.009	Y	0.04

Note. [[1]TA=Threat awareness (information), ATT=Attitude (personal motivation), SN=Subjective Norms (social motivation), SE=Self-efficacy(behavioural Skills), MF=Measures familiarity (behavioural Skills), SB = Security behaviour, Sig=Significance (at p<0.05)]

Table 6.6: Structural model statistics for IMB Skill Model constructs

	constructs	1	2	3	4	5	6
1	Measure Familiarity	1.00					
2	Security Attitude	0.43	1.00				
3	Security Behaviour	0.51	0.44	1.00			
4	Self-Efficacy	0.48	0.35	0.48	1.00		
5	Subjective Norm	0.12	0.06	0.10	0.14	1.00	
6	Threat Awareness	0.49	0.15	0.40	0.46	0.04	1.00

Note. p<0.05.

Table 6.7: Correlation matrix of IMB constructs

6.5. Discussion

This study examined the applicability of IMB Model in an HEI information security context, to study the factors affecting the security behaviours of the students. This study also studied the relationship of security awareness, which was measured in terms of threat awareness and familiarity with security measures, with security behaviour. Previously, this the relationship has been studied using PMT and TPB where only the indirect relationship of security awareness and security behaviours had been studied.

Our study showed that behavioural skills (both self-efficacy and measures familiarity) and personal motivation (attitude) directly predicted the security behaviour of the students. Also, the variables in the model explained 39% of the variance in security behaviour in our student sample. Furthermore, information and personal motivation were positively associated with behavioural skills (self-efficacy as well as security knowledge). We also found that information and personal motivation (represented by security attitude) indirectly affected security behaviour - through the behavioural skills (which operated as a mediator). Social motivation (captured in the form of subjective norms) did not have a direct or indirect relationship with security behaviour. Information and personal motivation variables also correlated with each other. However, no correlation was found between information and social motivation.

The results showed that threat awareness (information variable in the IMB model) directly predicted the security behaviour of the students. Threat awareness also turned out to be the most significant predictor for the self-efficacy and measures familiarity (both depicting behavioural skills).

Moreover, measures familiarity also had a significant relationship with security behaviour.

To evaluate our contribution to the study of information security in an educational context, two points need to be clarified beforehand. Specifically, our results need to be interpreted in the context of existing theory and previous findings. First, the difference between IMB Model and other known behavioural theories (TPB and PMT) is that IMB Model tends to explain behaviours directly, whereas, constructs of TPB and PMT influence behaviour through behavioural intention. Accordingly, we measured the predictors and mediator variables first and later followed up with the security behaviour measure (two weeks later). The first round of data collection and the subsequent time interval between the two parts of the survey may allow for a behavioural intention to form, like TPB and PMT, but we did not assess whether or not this was the case.

Second, our modified model shared two constructs with TPB and PMT, self-efficacy and attitude. While searching for reliable behavioural factors, Mayer et al. [15] found that self-efficacy has a reliable weak positive effect on behavioural intention in three different studies, whereas, in the case of TPB, the effect was medium. However, in the case of attitude measures, these have been shown to a reliable medium effect on behavioural intention in security studies. The results of our study confirmed the previous findings: self-efficacy had a small effect size on security behaviour (*f2=0.04*). However, in contrast to the medium effect reported for attitude [19], we found that attitude in our sample has a small effect size (*f2=0.11*) as well. As our results pertain to behaviour rather than intention, it is difficult to compare these effects directly. However, given the often noted disconnect between behavioural intention and behaviour (as intention may not always lead to behaviour), higher effect sizes may be expected for intention rather than behaviour which may not always align with one’s intention.

6.5.1. Recommendations

The previous two points lead us to the following recommendations for those responsible for managing information security training in HEIs. According to our results based on the IMB Model, constructs related to information (threat awareness) and motivation (based on attitudes and social norms) are crucial factors for students to acquire skills to engage in information security behaviours. However, practical knowledge is important in addition to information and motivation to employ security measures [17]. HEIs should focus on all three constructs, awareness, personal motivation and behavioural skills, simultaneously to improve the security behaviour of the students.

Training and other interventions based on the IMB Model may improve students' security-related knowledge by (a) increasing their access to information (e.g., through awareness campaigns), (b) raising their motivation (by increasing the perceived relevance and highlighting social norms supporting certain behaviours) and (c) providing them with opportunities to gain and test their behavioural skills. All three may then hopefully improve the security behaviours of the students in HEIs, reducing institutional vulnerability to threats while also giving the students the skills to act in a secure manner when they transition into the workplace and use employer systems.

6.5.2. Limitations and Future Research

The study is not without limitations. For example, our cross-sectional sample was recruited from a pool of students who enrolled in a security-related course. This suggests they may have been more interested in information security compared to those who selected other courses instead. Moreover, most of the students were bachelor level students belonging to computer science, information technology and engineering (STEM) disciplines. Therefore, our findings may not translate to students' behaviour outside these STEM areas that may lack threat knowledge and behavioural skills.

This leads us to three areas worthy of more investigation. One, more research is needed to establish the generalizability of our findings to other non-STEM samples. Two, it would be interesting to see the longitudinal effect of information, motivation and skills on security behaviour. We had a brief interval (two weeks) between our assessment of motivation, information and behavioural skill on the one hand, and security behaviour on the other. The relationship between the constructs may change over time, particularly if training is provided following the first round.

And three, security behaviour may be measured in numerous ways. A thoroughly designed construct may improve the predictability of the IMB Model. In this study, security behaviour was measured by asking participants to indicate which of the twelve security recommendations they follow (see also [44]). Moreover, information, knowledge and behaviour all were self-reported and may not depict the real level of threat awareness (information), knowledge (security measures) and behaviour. In future, the methods of measuring the actual information, knowledge and behaviour may be considered. If the study is replicated with the help of an IT support centre, for example, actual security behaviour may be captured by the IT system through the interaction of users with the system, circumventing the need for self-reported behavioural measures. The model may therefore also be of use to study security behaviour among other populations, such as employees and home-users.

6.6 Summary

In this study, we have examined the predictability of a slightly modified IMB Model in the context of security. The results of this study with 159 students showed that students with higher threat awareness, greater positive personal motivation, higher self-efficacy, and knowledge of security measures engaged in more secure behaviour. This work proves empirically that IMB model can be used to study security behaviours of the students.

Chapter 7

Conclusion

This chapter provides an overview of objectives as well as the key findings that are used to achieve the objectives and answer the research question.

The number of information security incidents reported in media and other sources is growing. To improve information security in organisations, both technical and non-technical measures are employed. Technical measures include (but not limited to) use of firewalls, backups, and anti-malware software, whereas, policies and security education, training and awareness (SETA) programs are used as non-technical measures to strengthen the users' ability to cope with the information security threats. SETA programs aim at increasing information security awareness (ISA) of the users and improve their security behaviour. ISA helps users in decision making in the event of a security incident, enhance understanding of possible threats, and make users familiarise with the countermeasures that can be employed to safeguard information security. However, despite all the effort, the weakest link's security behaviours are not improving.

Examination of literature suggests a lax in current SETA program's design. The SETA programs are designed as a one-fit-all solution, without involving users in the designing of such programs. Moreover, the said programs lack theory grounded approaches. While ISA has been proven to be one of the significant factors for improving security behaviour, the relationship requires a theory-grounded explanation, so that SETA programs are designed accordingly.

The studies presented in this thesis set out to improve the design of SETA programs by producing the knowledge that can be used to design SETA programs for students of higher education institutions (HEIs). The first study presented in chapter 3 this thesis identifies the weakest link in the weakest link, that is the groups of students who have a lower level of ISA, and needs training for improvement, by *describing the relationship of ISA with different individual factors of students* (***O₁***). The second study presented in chapter 4 of this thesis identifies the areas where students perceive to have security risks, by *identifying perceived information security concerns of the students* (***O₂***), so that such areas can be used in design SETA programs. The third study (chapter 5) examine the role of ISA in security behaviour by *describing difference between security behaviors of security experts, untrained students and trained students* (***O₃***); and finally, the fourth study (chapter 6) identifying the factors that should reflect in design of SETA program by *empirically testing a theoretical model explaining the relationship of ISA and security behaviour* (***O$_3$***).

Considering the breadth of the thesis, the outlined objectives cannot be achieved through a single methodology or a single wave of data collection. Empirical data for the objectives were collected through cross-sectional surveys. For each study, data were collected using online surveys, except for ***O$_2$*** where qualitative data was collected as part of the course assignment. The data for ***O$_1$,*** ***O$_2$*** and ***O$_3$*** were analysed using statistical techniques ranging from simple descriptive analysis to factor analysis in SPSS v24.0, and v25.0 whereas, data for ***O$_4$*** was analysed using structural equation modelling (SEM) in SmartPLS v3.0.

7.1 Thesis Summary and Key Findings

Each of the objectives as mentioned above is addressed in separate chapters.

Chapter 2 provided a review of relevant literature where two main themes are discussed: (1) On the understanding of information security awareness, and (2) theories used in studying security behaviours. The purpose of this chapter was to introduce readers to the concept of ISA and how it has been defined and assessed in the literature. Further, the introduction to the most popular theories used for studying information security behaviours was described. The review showed that the survey had been most often used as a tool to examine ISA. Most of the studies have assessed security awareness in general, and few took knowledge, attitude and behaviour into consideration. The review also showed that most of the security behavioural studies are focused on employees and that Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT), General Deterrence Theory (GDT) and Technology Acceptance Model (TAM) has been used in this context. The studies focused on students’ security behaviour mostly made use of TPB and PMT.

Chapter 3 describes an assessment study where ISA of students of different backgrounds was assessed, and a comparison of awareness was made among students divided based on their demographics, individual and cultural factors. The chapter provided insights on the ISA of the students. It was found that students believed that they have higher ISA level. However, an objective test of knowledge and examination of behaviour showed a different picture. It was found that male students had better ISA level as compared to female students. Younger students (under 21) were found to have lesser security awareness as compared to older students (21-40). IT students were found to be better in ISA comparison to students from other disciplines. The knowledge level differed across the disciplines. Finnish students were found better in security behaviours as compared to international students, and previous training was found to be a significant factor in better ISA as well. Thus, it can be concluded that students' awareness level different across different genders and educational disciplines. Moreover, young students and international students need improvement in their awareness as well.

Chapter 4 presents a two-phase study where a sequential Qual-Quan design was used for identifying and validating information security concerns of the students. The review a literature presented in this chapter showed that students are hardly involved in design of SETA program, and the studies most often assess the areas such as system security, email practices, threats, online services (including browsing and social networks), passwords, security policies, data security, device security (including smartphones) and information sharing habits. However, the findings from the two-phase study showed that students are concerned about their awareness of cyber laws, the risks arise due to their sociality i.e., their relationships with family and friends, and lapses at their university by the staff members. However, system security, web security, email security and passwords were the most prominent areas students were found concerned about.

Chapter 5 describes a comparative study where first security measures taken by the students are identified, along with data on their security practices. Next, a comparison of security practices was made with that of security experts to identify the gaps. Another purpose of this comparative study was to examine the role of ISA in security behaviours. While indeed students were found differences in their security practices in comparison with security experts, it was also found that students who had better awareness were somewhat similar in their practices to the security experts. And, even when knowledgeable students differ from the security experts, their deviating behaviour was not much of security risk.

Lastly, Chapter 6 presents an explanatory study where the relationship of security awareness and security behaviour is empirically validated. The results showed that information (awareness of threats), motivation (personal) and behavioural skills (self-efficacy and familiarity of security measures) are significant factors that affect security behaviour of the students.

7.2 Contributions and Implications

The research in this thesis makes significant contributions in information security research and has both theoretical and managerial implications.

7.2.1. Theoretical contributions

The objectives set for and achieved in this thesis are of interest to the researchers who are interested in understanding human behaviours related to information security. The work presented in this thesis extended the literature related to the human factor in information security in general and the role of students' information security in HEIs' information security, in particular.

For security researchers, firstly, the research shows that researchers should take personal, social and institutional dimensions into consideration as well when it comes to ISA studies. Currently, as evident from the literature, the focus of researchers is on technological and non-technological dimensions. Secondly, the research model tested in chapter 6 explains the relationship between ISA and security behaviours. Although the model used in the chapter mentioned above was not entirely supported (social support), it does prove the utility and applicability of a new behavioural model in information security research domain. Further research can use this finding as a starting point, test this model in different set up, on a different population, for example, to examine security behaviour of employees in the organisational set-up or that of home-users.

7.2.2. Managerial Implications

The research presented in this thesis provides exciting insights for security professionals who are responsible for managing information security in HEIs, as well as for the faculty members who design information security curricula and teach the students.

For information security professionals, who are responsible for protecting organisational information assets, this research provides insights into what are students' information security concerns, especially related to institutional dimension, and thus should take steps in ratifying them. This will, in turn, increase students' trust in the security measures implemented in HEIs. Further, the research also provides insights that can improve security professional's ability to tailor SETA programs by taking into account students' concerns, diversity in ISA level among different student groups, and the factors (awareness, motivation and skills) that affect the security behaviour.

For the faculty members, who design courses for the students, the research identifies the factors (awareness, motivation and skills) that can improve the security behaviour of the students. Thus, they can design a course focusing on improving their information, raising motivation and providing them with opportunities to gain and test their behavioural skills.

7.3 Limitations

The studies presented in this thesis are focused on information security of higher education institutions and have some limitations. A combination of previously validated instrument and self-designed instruments were used for the studies presented in this thesis. Reliability and validity of measures were checked where applicable. Moreover, attention check questions and quality checks were used to remove responses which could adversely affect the findings. Further, statistical analysis was used to remove incomplete responses and eliminate outliers. Despite all the efforts there exist some limitations to the work presented in this thesis.

The data was collected from a single case, using convenience sampling, due to non-availability to funds to collect census-representative data. The research was conducted in the

Department of Future Technologies, previously known as the Department of Information Technology and, therefore, most of the respondents were from IT, computer science or computer engineering backgrounds. Although data were collected from students of non-IT disciplines as well, they may not represent the whole student population of students from other disciplines. Moreover, many students work in addition to studying. This study looks at the information security issue in the context of educational institutions only, and therefore the participants were asked to consider themselves as students while answering the surveys.

The studies presented in this thesis are based on online (web-based) surveys. Such surveys are subject to self-selection bias [46] and may attract only those respondents who were comfortable with web-based surveys and have interest in the topic. Moreover, surveys provide a limited picture of what participants remember or what they are ready to share [47]. For the sake of this thesis, it is assumed that respondents of the studies have accurately reported their information security awareness, concerns and behaviours.

Considering that information security is a broad topic and many areas should be taken into consideration while assessing awareness and behaviours. Including all the areas in awareness assessment and security behaviour could lead to long surveys. The lengthy surveys not only adversely affect the response rate but also cause respondents to response without due attention. Therefore, I have been selective in picking area(s) in awareness and behaviour studies (Chapter 3, 5 and 6). I did not ask questions related to data security while comparing students' security practices with that of security experts due to non-availability of data. Moreover, some of the findings related to password management may become outdated when compared with the most recent to NIST guidelines for password management [254]. New guidelines do not consider changing password frequently and complex passwords as good security practices.

8. Bibliography

[1] J. C. Cronje, "The ABC (Aim, Belief, Concern) instant research question generator," Cape Peninsula University of Technology, Cape Town, 2012.

[2] G. Burrell, G. Morgan, and G. Morgan, *Sociological Paradigms and Organisational Analysis*. Routledge, 1979.

[3] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, Apr. 2016.

[4] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The Dark Side of the Internet: Attacks, Costs and Responses," *Inf. Syst.*, vol. 36, no. 3, pp. 675–705, 2011.

[5] E. Savitz, "Humans: The Weakest Link In Information Security," 2011. [Online]. Available: https://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/#77a4bb46de87. [Accessed: 11-Jun-2018].

[6] Z. Yan *et al.*, "Finding the Weakest Links in the Weakest Link: How Well do Undergraduate Students Make Cybersecurity Judgment?," *Comput. Human Behav.*, Feb. 2018.

[7] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technol. J.*, vol. 19, no. 3, pp. 122–131, 2001.

[8] Ponemon Institute, "2017 Cost of a Data Breach: global analysis," 2017 [Online]. Available: https://www.ibm.com/downloads/cas/ZYKLN2E3

[9] S. Aurigemma and R. Panko, "A Composite Framework for Behavioral Compliance with Information Security Policies," in *45th Hawaii International Conference on System Sciences*, 2012, pp. 3248–3257.

[10] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Q.*, vol. 34, pp. 523–548, 2010.

[11] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 2007, pp. 156b-156b.

[12] S. Abraham, "Information Security Behavior: Factors and Research Directions," in *AMCIS 2011*, 2011.

[13] D. W. Straub and R. J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Q.*, vol. 22, no. 4, p. 441, Dec. 1998.

[14] M. E. Thomson and R. von Solms, "Information security awareness: educating your users effectively," *Inf. Manag. Comput. Secur.*, vol. 6, no. 4, pp. 167–173, Oct. 1998.

[15] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Inf. Manag. Comput. Secur.*, vol. 8, no. 1, pp. 31–41, Mar. 2000.

[16] D.-L. Huang, P.-L. P. Rau, and G. Salvendy, "Perception of information security," *Behav. Inf. Technol.*, vol. 29, no. 3, pp. 221–232, May 2010.

[17] Q. Hu, T. Dinev, and T. Dinev, "Is spyware an Internet nuisance or

public menace?," *Commun. ACM*, vol. 48, no. 8, p. 61, Aug. 2005.

[18] N. Choi, D. Kim, J. Goo, and A. Whitmore, "Knowing is doing: An Empirical Validation of the Relationship between Managerial Information Security Awareness and Action," *Inf. Manag. Comput. Secur.*, vol. 16, no. 5, pp. 484–501, Nov. 2008.

[19] T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies ," *J. Assoc. Inf. Syst.*, vol. 8, no. 7, pp. 386–408, 2007.

[20] H. Kruger, T. Steyn, B. Dawn Medlin, and L. Drevin, "An Empirical Assessment of Factors Impeding Effective Password Management," *J. Inf. Priv. Secur.*, vol. 4, no. 4, pp. 45–59, Oct. 2008.

[21] V. Ahmed, "An Analysis of the Preparedness of Educational Institutions to Ensure the Security of Their Institutional Information," PhD Disseratation. School of Teaching, Learning and Leadership, University of Central Florida, 2018.

[22] Y. Levy and M. M. Ramim, "Towards an Evaluation of Cyber Risks and Identity Information Sharing Practices in e-Learning, Social Networking, and Mobile Texting Apps," in *Proceedings of 11th Chais Conference for the Study of Innovation and Learning Technologies:*, 2016, pp. 60E-69E.

[23] K. Wagataff and C. Sottile, "Cyberattack 101: Why Hackers Are Going After Universities," *NBC News*, 2015. [Online]. Available: https://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821. [Accessed: 10-Sep-2018].

[24] D. Storm, "Hacker breached 63 universities and government agencies | Computerworld," *ComputerWorld*, 2017. [Online]. Available: https://www.computerworld.com/article/3170724/security/hacker-breached-63-universities-and-government-agencies.html. [Accessed: 10-Sep-2018].

[25] The Guardian, "Australian National University 'hit by Chinese hackers' | Australia news | The Guardian," 2018. [Online]. Available: https://www.theguardian.com/australia-news/2018/jul/07/australian-national-university-hit-by-chinese-hackers. [Accessed: 10-Sep-2018].

[26] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Comput. Secur.*, vol. 27, no. 7, pp. 241–253, 2008.

[27] H. H. Cavusoglu *et al.*, "Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources," *Elsevier*, vol. 52, no. 4, pp. 385–400, Jun. 2015.

[28] N. F. Doherty, L. Anastasakis, and H. Fulford, "The information security policy unpacked: A critical study of the content of university policies," *Int. J. Inf. Manage.*, vol. 29, no. 6, pp. 449–457, Dec. 2009.

[29] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," *J. Comput. Inf. Syst.*, pp. 1–11, Mar. 2018.

[30] L. Hadlington and S. Chivers, "Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors," *Polic. A J. Policy Pract.*, Apr. 2018.

[31] L. Coleman and B. M. Purcell, "Data Breaches in Higher Education," *J. Bus. Cases Appl.*, vol. 15, 2015.

[32] Z. Tu and Y. Yuan, "Critical Success Factors Analysis on Effective

Information Security Management: A Literature Review," in *Twentieth Americans Conference on Information systems*, 2014.

[33] J. Zhang, B. J. Reithel, and H. Li, "Impact of perceived technical protection on security behaviors," *Inf. Manag. Comput. Secur.*, vol. 17, no. 4, pp. 330–340, Oct. 2009.

[34] L. Jaeger, "Information Security Awareness: Literature Review and Integrative Framework," in *51st Hawaii International Conference on System Sciences.*, 2018.

[35] B. Hanus and Y. "Andy" Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 2–16, Jan. 2016.

[36] R. Torten, C. Reaiche, and S. Boyle, "The impact of security awareness on information technology professionals' behavior," *Comput. Secur.*, Aug. 2018.

[37] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in Australian government organisations," *Inf. Manag. Comput. Secur.*, vol. 22, no. 4, pp. 334–345, Oct. 2014.

[38] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014.

[39] D. E. Gray, *Doing research in the real world*, 3rd ed. SAGE, 2014.

[40] E. Gummesson, "All research is interpretive!," *J. Bus. Ind. Mark.*, vol. 18, no. 6/7, pp. 482–492, Dec. 2003.

[41] M. B. Miles and A. M. Huberman, *Qualitative data analysis : an expanded sourcebook*. Sage Publications, 1994.

[42] C. Perry and O. Jensen, "Approaches to Combining Induction and Deduction In One Research Study," in *In Conference of the Australian and New Zealand Marketing Academy, Auckland, New Zealand.*, 2001.

[43] M. Crotty, *The foundations of social research : meaning and perspective in the research process*. Sage Publications, 1998.

[44] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 3rd ed. SAGE Publications, 2009.

[45] E. Babbie, *The Practice of Social Research*, 13th ed. WADSWORTH CENGAGE Learning, 2013.

[46] L. M. Rea and R. A. (Richard A. Parker, *Designing and conducting survey research : a comprehensive guide*, 1st ed. John Wiley & Sons, 2014.

[47] P. M. Nardi, *Doing Survey Research: A guide to Quantitative Methods*. Routledge, 2018.

[48] M. Siponen, "Five dimensions of information security awareness," *ACM SIGCAS Comput. Soc.*, vol. 31, no. 2, pp. 24–29, Jun. 2001.

[49] F. Häußinger, "Studies on Employees' Information Security Awareness," Niedersächsische Staats-und Universitätsbibliothek Göttingen, 2015.

[50] A. H. Maslow, "A theory of human motivation.," *Psychol. Rev.*, vol. 50, no. 4, pp. 370–396, 1943.

[51] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," in *2013 International Conference on Availability, Reliability and Security*, 2013, pp. 546–555.

[52] N. V. Olijnyk, "A quantitative examination of the intellectual profile and

evolution of information security from 1965 to 2015," *Scientometrics*, vol. 105, no. 2, pp. 883–904, Nov. 2015.

[53] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[54] A. Tsohou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "Investigating Information Security Awareness: Research and Practice Gaps," *Inf. Secur. J. A Glob. Perspect.*, vol. 17, no. 5–6, pp. 207–227, Dec. 2008.

[55] C. Banerjee, A. Banerjee, and P. D. Murarka, "An Improvised Software Security Awareness Model," *Int. J. Information, Commun. Comput. Technol.*, no. II, pp. 43–48, 2013.

[56] C. Banerjee and S. K. Pandey, "Research on software security awareness," *ACM SIGSOFT Softw. Eng. Notes*, vol. 35, no. 5, p. 1, Oct. 2010.

[57] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterence Approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, Mar. 2009.

[58] J. D 'arcy and A. Hovav, "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *J. Bus. Ethics*, vol. 89, pp. 59–71, 2009.

[59] T. Dinev, J. Goo, Q. Hu, and K. Nam, "User behaviour towards protective information technologies: the role of national cultural differences," *Inf. Syst. J.*, vol. 19, no. 4, pp. 391–412, Jul. 2009.

[60] S. M. Galvez and I. R. Guzman, "Identifying Factors that Influence Corporate Information Security Behavior," in *Proceedings of 15th American Conference on Information Systems*, 2009, p. 765.

[61] E. Kritzinger and E. Smith, "Information security management: An information security retrieval and awareness model for industry," *Comput. Secur.*, vol. 27, no. 5–6, pp. 224–231, Oct. 2008.

[62] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Roles of information security awareness and perceived fairness in information security policy compliance," in *15th Americas Conference on Information Systems 2009, AMCIS 2009*, 2009, vol. 5, pp. 3269–3277.

[63] J. Spears and H. Barki, "User Participation in Information Systems Security Risk Management," *MIS Q.*, vol. 34, no. 3, p. 503, 2010.

[64] F. Hellquist, S. Ibrahim, R. Jatko, and A. Andersson, "Getting their Hands Stuck in the Cookie Jar - Students' Security Awareness in 1:1 Laptop Schools," *Int. J. public Inf. Syst.*, vol. 9, no. 1, pp. 1–18, 2013.

[65] J. S. Lim *et al.*, "Embedding Information Security Culture Emerging Concerns and Challenges," in *PACIS*, 2010, p. 43.

[66] B. Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, Mar. 2009.

[67] T. R. Peltier, "Implementing an Information Security Awareness Program," *Inf. Syst. Secur.*, vol. 14, no. 2, pp. 37–49, 2005.

[68] N. H. A. Rahim, S. Hamid, M. L. Mat Kiah, S. Shamshirband, and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes*, vol. 44, no. 4, pp. 606–622, Apr. 2015.

[69] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[70] M. van der Walt, K. Maree, and S. Ellis, "A Mathematics Vocabulary

Questionnaire for Use in the Intermediate Phase," *South African J. Educ.*, vol. 28, pp. 489–504, 2008.

[71] S. M. Furnell, P. Bryant, and A. D. Phippen, "Assessing the security perceptions of personal Internet users," *Comput. Secur.*, vol. 26, no. 5, pp. 410–417, Aug. 2007.

[72] S. Talib, N. L. Clarke, and S. M. Furnell, "An Analysis of Information Security Awareness within Home and Work Environments," in *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 196–203.

[73] E. B. Kim, "Information Security Awareness Status of Business College: Undergraduate Students," *Inf. Secur. J. A Glob. Perspect.*, vol. 22, no. 4, pp. 171–179, Jul. 2013.

[74] L. Slusky and P. Partow-Navid, "Students Information Security Practices and Awareness.," *J. Inf. Priv. Secur.*, vol. 8, no. 4, pp. 3–26, 2012.

[75] E. M. Power, "Developing a Culture of Privacy: A Case Study," *IEEE Secur. Priv. Mag.*, vol. 5, no. 6, pp. 58–60, Nov. 2007.

[76] K. Rantos, K. Fysarakis, and C. Manifavas, "How Effective Is Your Security Awareness Program? An Evaluation Methodology," *Inf. Secur. J. A Glob. Perspect.*, vol. 21, no. 6, pp. 328–345, Jan. 2012.

[77] D. Mani, S. Mubarak, and K. Choo, "Understanding the information security awareness process in real estate organizations using the SECI model," 2014.

[78] L. Drevin, H. A. Kruger, and T. Steyn, "Value-focused assessment of ICT security awareness in an academic environment," *Comput. Secur.*, vol. 26, no. 1, pp. 36–43, Feb. 2007.

[79] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Inf. Manag. Comput. Secur.*, vol. 18, no. 5, pp. 316–327, Nov. 2010.

[80] E. Albrechtsen, "A qualitative study of users' view on information security," *Comput. Secur.*, vol. 26, no. 4, pp. 276–289, Jun. 2007.

[81] S. Furman, M. F. Theofanos, Y.-Y. Choong, and B. Stanton, "Basing Cybersecurity Training on User Perceptions," *IEEE Secur. Priv. Mag.*, vol. 10, no. 2, pp. 40–49, Mar. 2012.

[82] C. C. Chen, R. S. Shaw, and S. C. Yang, "Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System," *Inf. Technol. Learn. Perform. J.*, vol. 24, no. 1, 2006.

[83] D. Charoen, M. Raman, and L. Olfman, "Improving End User Behaviour in Password Utilization: An Action Research Initiative," *Syst. Pract. Action Res.*, vol. 21, no. 1, pp. 55–72, Feb. 2008.

[84] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Comput. Secur.*, vol. 26, no. 1, pp. 63–72, Feb. 2007.

[85] W. A. Labuschagne, I. Burke, N. Veerasamy, and M. M. Eloff, "Design of cyber security awareness game utilizing a social media framework," in *2011 Information Security for South Africa*, 2011, pp. 1–9.

[86] E. Kritzinger and S. H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Comput. Secur.*, vol. 29, no. 8, pp. 840–847, Nov. 2010.

[87] J. Hagen, E. Albrechtsen, and S. Ole Johnsen, "The long-term effects of information security e-learning on organizational learning," *Inf. Manag.*

Comput. Secur., vol. 19, no. 3, pp. 140–154, Jul. 2011.

[88] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going Spear Phishing: Exploring Embedded Training and Awareness," *IEEE Secur. Priv.*, vol. 12, no. 1, pp. 28–38, Jan. 2014.

[89] G. Salvendy, *Handbook of human factors and ergonomics*, 4th ed. John Wiley & Sons, 2012.

[90] N. Lim, "Consumers' perceived risk: sources versus consequences," *Electron. Commer. Res. Appl.*, vol. 2, no. 3, pp. 216–228, Sep. 2003.

[91] W.-J. Jih, S.-Y. Wong, and T.-B. Chang, "Effects of Perceived Risks on Adoption of Internet Banking Services," *Int. J. E-bus. Res.*, vol. 1, no. 1, pp. 70–88, Jan. 2005.

[92] M. S. Featherman and P. A. Pavlou, "Predicting e-services adoption: a perceived risk facets perspective," *Int. J. Hum. Comput. Stud.*, vol. 59, no. 4, pp. 451–474, Oct. 2003.

[93] K.-L. Thomson and R. von Solms, "Information security obedience: a definition," *Comput. Secur.*, vol. 24, no. 1, pp. 69–75, Feb. 2005.

[94] S. Chai, S. Bagchi-Sen, C. Morrell, H. R. Rao, and S. Upadhyaya, "Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children's Information Security Behavior," *Issues Informing Sci. Inf. Technol.* , vol. 3, 2006.

[95] A. Stewart, "On risk: perception and direction," *Comput. Secur.*, vol. 23, no. 5, pp. 362–370, Jul. 2004.

[96] K. Aytes and T. Connolly, "Computer Security and Risky Computing Practices," *J. Organ. End User Comput.*, vol. 16, no. 3, pp. 22–40, Jul. 2004.

[97] K. Aytes and T. Conolly, "A Research Model for Investigating Human Behavior Related to Computer Security," in *Americas Conference on Information Systems (AMCIS)*, 2003, p. 260.

[98] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The Psychology of Security for the Home Computer User," in *2012 IEEE Symposium on Security and Privacy*, 2012, pp. 209–223.

[99] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Comput. Secur.*, vol. 56, pp. 83–93, Feb. 2016.

[100] S. Mishra and G. Dhillon, "Information Systems Security Governance Research: A Behavioral Perspective," in *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, 2006.

[101] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, Feb. 2013.

[102] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: a theory-based literature review," *Manag. Res. Rev. Inf. Manag. Comput. Secur. Iss Comput. Secur. Iss*, vol. 37, no. 4, pp. 1049–1092, 2014.

[103] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance," *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 42–75, Mar. 2014.

[104] P. Mayer, A. Kunz, and M. Volkamer, "Reliable Behavioural Factors in the Information Security Context," in *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17*, 2017, pp. 1–10.

[105] I. Ajzen and M. Fishbein, *Understanding attitudes and predicting social behavior*. Prentice-Hall, 1980.

[106] M. Fishbein and I. Ajzen, *Belief, attitude, intention, and behavior : an introduction to theory and research*. Addison-Wesley Pub. Co, 1975.

[107] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, Dec. 1991.

[108] A. Al-Omari, O. El-Gayar, and A. Deokar, "Security Policy Compliance: User Acceptance Perspective," in *2012 45th Hawaii International Conference on System Sciences*, 2012, pp. 3317–3326.

[109] S. Bauer and E. W. N. Bernroider, "From Information Security Awareness to Reasoned Compliant Action," *ACM SIGMIS Database DATABASE Adv. Inf. Syst.*, vol. 48, no. 3, pp. 44–68, Aug. 2017.

[110] S. Bauer and E. W. N. Bernroider, "The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2015, pp. 154–164.

[111] F. F. Putri and A. Hovav, "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory," *Proc. ECIS*, Jun. 2014.

[112] A. Yazdanmehr and J. Wang, "Employees' information security policy compliance: A norm activation perspective," *Decis. Support Syst.*, vol. 92, pp. 36–46, Dec. 2016.

[113] S. H. Schwartz, "Normative Influences on Altruism," *Adv. Exp. Soc. Psychol.*, vol. 10, pp. 221–279, Jan. 1977.

[114] N. Kumar, K. Mohan, and R. Holowczak, "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls," *Decis. Support Syst.*, vol. 46, no. 1, pp. 254–264, Dec. 2008.

[115] D. Meichenbaum and D. C. Turk, *Facilitating treatment adherence: A practitioner's guidebook*. New York, NY, US: Plenum Press, 1987.

[116] J. D'Arcy and A. Hovav, "Deterring internal information systems misuse," *Commun. ACM*, vol. 50, no. 10, pp. 113–117, Oct. 2007.

[117] A. Hovav and J. D'Arcy, "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea," *Inf. Manag.*, vol. 49, no. 2, pp. 99–110, Mar. 2012.

[118] J. D. Fisher and W. A. Fisher, "Changing AIDS-risk behavior," *Psychol. Bull.*, vol. 111, no. 3, pp. 455–474, 1992.

[119] J. D. Fisher, W. A. Fisher, S. J. Misovich, D. L. Kimble, and T. E. Malloy, "Changing AIDS risk behavior: Effects of an intervention emphasizing AIDS risk reduction information, motivation, and behavioral skills in a college student population.," *Heal. Psychol.*, vol. 15, no. 2, pp. 114–123, 1996.

[120] A. A. Robertson, J. A. Stein, and C. Baird-Thomas, "Gender differences in the prediction of condom use among incarcerated juvenile offenders: testing the information-motivation-behavior skills (IMB) model," *J. Adolesc. Heal.*, vol. 38, no. 1, pp. 18–25, Jan. 2006.

[121] W. A. Fisher, S. S. Williams, J. D. Fisher, and T. E. Malloy, "Understanding AIDS Risk Behavior Among Sexually Active Urban Adolescents: An Empirical Test of the Information–Motivation–Behavioral Skills Model," *AIDS Behav.*, vol. 3, no. 1, pp. 13–23, 1999.

[122] J. D. Fisher, W. A. Fisher, and J. J. Harman, "An Information-

Motivation-Behavioral Skills Model of Adherence to Antiretroviral Therapy," *Heal. Psychol.*, vol. 25, no. 4, pp. 462–473, 2006.

[123] D. E. Glasford, "Predicting Voting Behavior of Young Adults: The Importance of Information, Motivation, and Behavioral Skills," *J. Appl. Soc. Psychol.*, vol. 38, no. 11, pp. 2648–2672, Nov. 2008.

[124] J. D. Seacat and D. Northrup, "An information–motivation–behavioral skills assessment of curbside recycling behavior," *J. Environ. Psychol.*, vol. 30, no. 4, pp. 393–401, Dec. 2010.

[125] B. Khan, K. S. Alghathbar, and M. K. Khan, "Information Security Awareness Campaign: An Alternate Approach," in *International Conference on Information Security and Assurance*, 2011, pp. 1–10.

[126] M. G. Mariani and S. Zappalà, "PC Virus Attacks in Small Firms: Effects of Risk Perceptions and Information Technology Competence on Preventive Behaviors," *TPM Testing, Psychom. Methodol. Appl. Psychol.*, vol. 21, no. 1, pp. 51–65, 2014.

[127] R. E. Crossler and F. Bélanger, "The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors," in *50th Hawaii International Conference on System Sciences*, 2017.

[128] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, Sep. 1983.

[129] T. Sommestad, H. Karlzen, and J. Hallberg, "The Theory of Planned Behavior and Information Security Policy Compliance," *J. Comput. Inf. Syst.*, pp. 1–10, 2017.

[130] M. R. Pattinson, G. Anderson, and A. Analyses, "End-user Risk-taking Behaviour: an application of the IMB model," in *6th Annual Security Conference*, 2007.

[131] G. R. Donenberg, R. M. Schwartz, E. Emerson, H. W. Wilson, F. B. Bryant, and G. Coleman, "Applying a Cognitive-Behavioral Model of HIV Risk to Youths in Psychiatric Care," *AIDS Educ. Prev.*, vol. 17, no. 3, pp. 200–216, Jun. 2005.

[132] T. Chang *et al.*, "A study on the Information-Motivation-Behavioral Skills Model among Chinese Adults with Peritoneal Dialysis," *J. Clin. Nurs.*, vol. 27, no. 9–10, pp. 1884–1890, Feb. 2018.

[133] W. A. Fisher, T. Kohut, H. Schachner, and P. Stenger, "Understanding Self-Monitoring of Blood Glucose Among Individuals With Type 1 and Type 2 Diabetes," *Diabetes Educ.*, vol. 37, no. 1, pp. 85–94, Jan. 2011.

[134] C. H. Talley, L. Yang, and K. P. Williams, "Breast Cancer Screening Paved with Good Intentions: Application of the Information–Motivation–Behavioral Skills Model to Racial/Ethnic Minority Women," *J. Immigr. Minor. Heal.*, vol. 19, no. 6, pp. 1362–1371, Dec. 2017.

[135] T. Fullerton, B. J. Rye, G. Meaney, and C. Loomis, "Condom and Hormonal Contraceptive Use by Young Women: An Information-Motivation-Behavioral Skills Assessment," *Can. J. Behav. Sci.*, vol. 45, no. 3, pp. 196–209, 2013.

[136] C. Colwill, "Human factors in information security: The insider threat – Who can you trust these days?," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, Nov. 2009.

[137] S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," *Comput. Secur.*, vol. 25, no. 1, pp. 27–35, Feb. 2006.

[138] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, May 2009.

[139] C. Vroom and R. von Solms, "Towards information security behavioural compliance," *Comput. Secur.*, vol. 23, no. 3, pp. 191–198, May 2004.

[140] J. Frederick Van Niekerk, "Establishing An Information Security Culture in Organizations: An Outcomes based Education Approach," Nelson Mandela Metropolitan University, 2005.

[141] W. H. DeLone and E. R. McLean, "Information Systems Success: The Quest for the Dependent Variable," *Inf. Syst. Res.*, vol. 3, no. 1, pp. 60–95, Mar. 1992.

[142] P. Spurling, "Promoting security awareness and commitment," *Inf. Manag. Comput. Secur.*, vol. 3, no. 2, pp. 20–26, May 1995.

[143] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' Information Security Awareness and Behavior: A Literature Review," in *46th Hawaii International Conference on System Sciences*, 2013, pp. 2978–2987.

[144] E. B. Kim, "Recommendations for information security awareness training for college students," *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 115–126, Mar. 2014.

[145] D. J. Kuss and M. D. Griffiths, "Online Social Networking and Addiction—A Review of the Psychological Literature," *Int. J. Environ. Res. Public Health*, vol. 8, no. 9, pp. 3528–3552, Aug. 2011.

[146] F. H. Katz, "The Effect of a University Information Security Survey on Instruction Methods in Information Security," in *Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05*, 2005, p. 43.

[147] B. L. Ingerman and C. Yang, "Top-Ten IT Issues, 2011.," *Educ. Rev.*, vol. 46, no. 3, p. 24, 2011.

[148] H.-J. Kam and P. Katerattanakul, "Information Security in Higher Education: A Neo-Institutional Perspective," *J. Inf. Priv. Secur.*, vol. 10, no. 1, pp. 28–43, Jan. 2014.

[149] H. Chan and S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector," *Int. J. Comput. Appl.*, vol. 60, no. 10, pp. 975–8887, 2012.

[150] R. D. Butler, "An Examination of Issues Surrounding Information in California Colleges," Northcentral University, 2013.

[151] S. Braman, "Defining information: An approach for policymakers," *Telecomm. Policy*, vol. 13, no. 3, pp. 233–242, Sep. 1989.

[152] C. P. Pfleeger and S. L. Pfleeger, *Security in computing*. Prentice Hall PTR, 2003.

[153] M. E. Whitman and H. J. Mattord, *Principles of information security*, 4th ed. Cengage Learning, 2012.

[154] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*. Pearson, 2006.

[155] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 2014, pp. 248–252.

[156] S. K. Katsikas, "Health care management and information systems

security: awareness, training or education?," *Int. J. Med. Inform.*, vol. 60, no. 2, pp. 129–135, Nov. 2000.

[157] M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program Technology Administration," 2003.

[158] W. A. Al-Hamdani and W. A., "Assessment of need and method of delivery for information security awareness program," in *Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD '06*, 2006, p. 102.

[159] Deloitte, "Raising the Bar 2011 TMT Global Security Study-Key Findings," 2011.

[160] PWC, "Changing the game Key findings from The Global State of Information Security® Survey 2013," 2013.

[161] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, Apr. 2009.

[162] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Comput. Secur.*, vol. 24, no. 2, pp. 124–133, 2005.

[163] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," *Computer (Long. Beach. Calif).*, vol. 43, no. 2, pp. 64–71, Feb. 2010.

[164] H. A. Kruger, L. Drevin, S. Flowerday, and T. Steyn, "An assessment of the role of cultural factors in information security awareness," in *2011 Information Security for South Africa*, 2011, pp. 1–7.

[165] I. V. S. Mullis, M. O. Martin, and P. Foy, *IEA's TIMSS 2003 international report on achievement in the mathematics cognitive domains: findings from a developmental project*. Chestnut Hill, MA: TIMSS & PIRLS International Study Center, Lynch School of Education, Boston College, 2005.

[166] A. J. Mills, G. Durepos, and E. Wiebe, *Encyclopedia of case study research*. SAGE, 2010.

[167] P. Tarwireyi, S. Flowerday, and A. Bayaga, "Information Security Competence Test with Regards to Password Management," in *Information Security South Africa (ISSA)*, 2011.

[168] D. A. Dillman, *Mail and Internet Surveys The Tailored Design Method*. Wiley, J, 2011.

[169] R. S. Mansfield, "Building competency models: Approaches for HR professionals," *Hum. Resour. Manage.*, vol. 35, no. 1, pp. 7–18, 1996.

[170] UTU, "Study Statistics of the University of Turku," 2015. [Online]. Available: http://www.utu.fi/en/university/key-figures/study-statistics/Pages/home.aspx. [Accessed: 20-Mar-2015].

[171] Y. Li and M. Siponen, "A Call For Research On Home Users' Information Security Behaviour," in *Pacific Asia Conference on Information Systems (PACIS)*, 2011, vol. 112.

[172] N. Thompson, T. J. McGill, and X. Wang, "'Security begins at home': Determinants of home computer and mobile device security behavior," *Comput. Secur.*, vol. 70, pp. 376–391, 2017.

[173] C. S. Abraham, P. Sheeran, D. Abrams, and R. Spears, "Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of hiv infection," *Psychol. Health*, vol. 9, no. 4, pp. 253–272, May 1994.

[174] C. Yoon, J.-W. J.-W. Hwang, and R. Kim, "Exploring Factors that

Influence Students' behaviors in Information Security," *J. Inf. Syst. Educ.*, vol. 23, no. 4, pp. 407–415, 2012.

[175] I. Woon, G.-W. Tan, R. Low, I. M. Y. Woon, G. W. Tan, and R. T. Low, "A Protection Motivation Theory Approach to Home Wireless Security," in *International Conference on Information Systems (ICIS)*, 2005.

[176] B. Kerievsky and Bruce, "Security and Confidentiality in a University Computer Network," *ACM SIGUCCS Newsl.*, vol. 6, no. 3, pp. 9–11, Sep. 1976.

[177] F. A. Aloul, "Informa tion Security Awareness in UAE: A survey paper," in *2010 International Conference for Internet Technology and Secured Transactions.*, 2010, pp. 1–6.

[178] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Comput. Secur.*, vol. 31, no. 8, pp. 983–988, Nov. 2012.

[179] M. T. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions," *ACM SIGMIS Database*, vol. 38, no. 1, p. 60, Feb. 2007.

[180] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Comput. Human Behav.*, vol. 69, pp. 151–156, Apr. 2017.

[181] A. Farooq and S. R. U. Kakakhel, "Information security awareness: Comparing perceptions and training preferences," in *Conference Proceedings - 2013 2nd National Conference on Information Assurance, NCIA 2013*, 2013, pp. 53–57.

[182] S. Loucks-Horsley, *Designing professional development for teachers of science and mathematics*. Corwin Press, 2010.

[183] G. R. Milne, L. I. Labrecque, and C. Cromer, "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices," *J. Consum. Aff.*, vol. 43, no. 3, pp. 449–473, Sep. 2009.

[184] L. J. Camp, "Mental models of privacy and security," *IEEE Technol. Soc. Mag.*, vol. 28, no. 3, pp. 37–46, 2009.

[185] A. Marks, "Exploring Universities' Information Systems Security Awareness in a Changing Higher Education Environment : A Comparative Case Study Research," University of Salford, 2007.

[186] Y. Wu, F. K. Andoh-baidoo, R. Crossler, and J. Tanguma, "An Exploratory Study of the Security Management Practices of Hispanic Students," *Int. J. Secur.*, vol. 5, no. 1, pp. 13–21, 2011.

[187] C. D. Schou and K. J. Trimmer, "Information Assurance and Security," *J. Organ. End User Comput.*, vol. 16, no. 3, 2004.

[188] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Comput. Secur.*, vol. 34, pp. 47–66, May 2013.

[189] R. E. Crossler, F. Bélanger, and D. Ormond, "The quest for complete security: An empirical analysis of users' multi-layered protection from security threats," *Inf. Syst. Front.*, pp. 1–15, Apr. 2017.

[190] A. Farooq *et al.*, "Dimensions of Internet Use and Threat Sensitivity: An Exploratory Study among Students of Higher Education," in *2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES)*, 2016, pp. 534–541.

[191] V. Cambazoglu and N. Thota, "Computer Science Students' Perception

of Computer Network Security," in *2013 Learning and Teaching in Computing and Engineering*, 2013, pp. 204–207.

[192] L. Mensch, Scott; Wilkie, "Information Security Activities of College Students: An Exploratory Study," *Acad. Inf. Manag. Sci.*, vol. 14, no. 2, pp. 91–116, 2011.

[193] J. Morgan, J.-M. Maris, and A. C. Lorents, "Security Practices of Students," in *24th Information Systems Education Conference, ISECON*, 2007.

[194] B. Ngoqo and S. V Flowerday, "Student Information Security Behavioral Intent: Assessing the Actions and Intentions of Students in a Developmental University," in *ICERI2014: 7th International Conference of Education, Research and Innovation*, 2014, pp. 3524–3532.

[195] F. P. Teer, S. E. Kruck, and G. P. Kruck, "Empiracal Study of Students' Computer Security Practices/Perceptions," *J. Comput. Inf. Syst.*, vol. 4417, no. 15, pp. 105–110, 2007.

[196] Y. Yunus and Z. F. Zamzuri, "Assessing the Students' Awareness in Information Security Threats in E-Learning : a Case Study," in *The Second International Conference on Digital Enterprise and Information Systems (DEIS2013)*, 2013, pp. 194–199.

[197] R. Crossler, M. A. Villarreal, and F. K. Andoh-Baidoo, "A preliminary study examining the security practices of hispanic college students," 2011.

[198] C. P. Garrison and O. G. Posey, "Computer Security Awareness of Accounting Students," in *Southwest Decision Sciences Thirty-Sixth Annual Meeting*, 2006.

[199] H. Hamid and A. M. Zeki, "Users' Awareness of and Perception on Information Security Issues: A Case Study of Kulliyyah of ICT Postgraduate Students," in *2014 3rd International Conference on Advanced Computer Science Applications and Technologies*, 2014, pp. 139–144.

[200] M. A. Harris, S. Furnell, and K. Patten, "Comparing the Mobile Device Security Behavior of College Students and Information Technology Professionals," *J. Inf. Priv. Secur.*, vol. 10, no. 4, pp. 186–202, Oct. 2014.

[201] E. Lomo-david and L. J. Shannon, "Information Systems Security and Safety Measures : the Dichotomy Between Students ' Familiarity and Practice," *Acad. Informait. Manag. Sci. J.*, vol. 12, no. 1, pp. 1–4, 2009.

[202] E. Lomo-David, A. Acılar, B. F. Chapman, and L.-J. Shannon, "University Students Computer Security Practices in Two Developing Nations: A Comparative Analysis," in *Third Annual General Business Conference Proceedings*, 2011, pp. 167–180.

[203] H. Abdul Majid, M. Abdul Majid, M. I. Ibrahim, W. N. S. Wan Manan, and M. R. Ramli, "Investigation of security awareness on e-learning system among lecturers and students in Higher Education Institution," in *2015 International Conference on Computer, Communications, and Control Technology (I4CT)*, 2015, pp. 216–220.

[204] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Observations on Genderwise Differences among University Students in Information Security Awareness," *Int. J. Inf. Secur. Priv.*, vol. 9, no. 2, pp. 60–74, Apr. 2015.

[205] A. Farooq, J. J. Isoaho, S. Virtanen, and J. J. Isoaho, "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors," in *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 2015, vol. 1, pp. 352–359.

[206] M. A. Harris, S. Furnell, and K. Patten, "Comparing the Mobile Device Security Behavior of College Students and Information Technology Professionals," *J. Inf. Priv. Secur.*, vol. 10, no. 4, pp. 186–202, Oct. 2014.

[207] V. Stanciu and A. Tinca, "Students' awareness on information security between own perception and reality – an empirical study," *Account. Manag. Inf. Syst.*, vol. 15, no. 1, pp. 112–130, 2016.

[208] M. Aliyu, N. A. O. Abdallah, N. A. Lasisi, D. Diyar, and A. M. Zeki, "Computer security and ethics awareness among IIUM students: An empirical study," in *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*, 2010, pp. A52–A56.

[209] J. Ryan and J. Ryan, "Information security awareness: An evaluation among business students with regard to computer self-efficacy and personal innovation," in *AMCIS 2007 Proceedings*, 2007, pp. 12–31.

[210] S. A. Shonola and M. S. Joy, "Mobile learning security concerns from university students' perspectives," in *2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014)*, 2014, pp. 165–172.

[211] R. Barberet and B. S. Fisher, "Can security beget insecurity? Security and crime prevention awareness and fear of burglary among university students in the East Midlands," *Secur. J.*, vol. 22, no. S1, pp. 3–23, Feb. 2009.

[212] I. Androulidakis and G. Kandus, "Bluetooth® usage among students as an indicator of security awareness and feeling - IEEE Xplore Document," in *2011 Proceedings of ELMAR*, 2011, pp. 157–160.

[213] B. H. Jones, A. G. Chin, and P. Aiken, "Risky business: Students and smartphones," *TechTrends*, vol. 58, no. 6, pp. 73–83, Nov. 2014.

[214] W. M. Trochim, "Research Methods Knowledge Base," 2001. [Online]. Available: http://www.anatomyfacts.com/research/researchmethodsknowledgebase.pdf. [Accessed: 06-Dec-2016].

[215] J. G. Nouria Bricki, "A Guide to Using Qualitative Research Methodology," 2007.

[216] S. Kraemer, P. Carayon, and J. Clem, "Human and organizational factors in computer and information security: Pathways to vulnerabilities," *Comput. Secur.*, vol. 28, no. 7, pp. 509–520, 2009.

[217] A. B. Osborne, Jason W., Costello, "Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis.," *Pan-Pacific Manag. Rev.*, vol. 12, no. 2, pp. 131–146, 2009.

[218] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *IEEE Symposium on Security and Privacy*, 1997, pp. 154–163.

[219] J. He and F. J. R. van de Vijver, "Self-presentation styles in self-reports: Linking the general factors of response styles, personality traits, and values in a longitudinal study," *Pers. Individ. Dif.*, vol. 81, pp. 129–134, Jul. 2015.

[220] A. Mathur, N. Malkin, M. Harbach, E. Peer, and S. Egelman, "Quantifying Users' Beliefs about Software Updates," in *Network and Distributed Systems Security (NDSS) Symposium*, 2018.

[221] E. Pettersson *et al.*, "Do maladaptive behaviors exist at one or both ends of personality traits?," *Psychol. Assess.*, vol. 26, no. 2, pp. 433–446, 2014.

[222] H. Suh, N. Shahriaree, E. B. Hekler, and J. A. Kientz, "Developing and Validating the User Burden Scale," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 2016, pp. 3988–3999.

[223] L. R. Fabrigar, D. T. Wegener, R. C. Maccallum, and E. J. Strahan, "Evaluating the Use of Exploratory Factor Analysis in Psychological Research," *Psychol. Methods*, vol. 4, no. 3, pp. 272–299, 1999.

[224] Ponemon, "2013 State of the Endpoint," Michigan, 2012.

[225] F. Mwagwabi, T. McGill, and M. Dixon, "Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines," in *47th Hawaii International Conference on System Sciences (HICSS)*, 2014, pp. 3188–3197.

[226] M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," *Heal. Inf. Libr. J.*, vol. 26, no. 2, pp. 91–108, Jun. 2009.

[227] R. Reeder, I. Ion, and S. Consolvo, "152 Simple Steps to Stay Safe Online: Security Advice for Non-tech-savvy Users," *IEEE Secur. Priv.*, no. 99, 2017.

[228] I. Ion, R. Reeder, and S. Consolvo, "'...no one can hack my mind': Comparing Expert and Non-Expert Security Practices," in *2015 Symposium on Usable Privacy and Security*, 2015, pp. 327–340.

[229] A. Langley, "Strategies for Theorizing from Process Data," *Acad. Manag. Rev.*, vol. 24, no. 4, p. 691, Oct. 1999.

[230] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed. L. Erlbaum Associates, 1988.

[231] S. Al-Janabi and I. Al-Shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," *J. Inf. Knowl. Manag.*, vol. 15, no. 01, p. 1650007, Mar. 2016.

[232] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975.

[233] T. Sommestad, H. Karlzén, and J. Hallberg, "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour," *Int. J. Inf. Secur. Priv.*, vol. 9, no. 1, 2015.

[234] M. Chesaniuk, H. Choi, P. Wicks, and G. Stadler, "Perceived stigma and adherence in epilepsy: Evidence for a link and mediating processes," *Epilepsy Behav.*, vol. 41, pp. 227–231, Dec. 2014.

[235] H. Van Nguyen, T. T. Vu, and H. N. Pham, "Factors Associated with Drug Use Among Male Motorbike Taxi Drivers in Urban Vietnam," *Subst. Use Misuse*, vol. 49, no. 10, pp. 1287–1295, Aug. 2014.

[236] B. K. Kim, H. S. Jo, and H. J. Lee, "Study on the Factors Related With Intention of Cancer Screening Among Korean Residents," *Asia Pacific J. Public Heal.*, vol. 27, no. 2, pp. NP2133–NP2143, Mar. 2015.

[237] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "'My Data Just Goes Everywhere': User Mental Models of the Internet and Implications for Privacy and Security," in *Symposium on Usable Privacy and Security*

(SOUPS), 2015, pp. 39–52.

[238] A. Farooq, S. R. U. Kakakhel, S. Virtanen, and J. Isoaho, "A taxonomy of perceived information security and privacy threats among IT security students," in *10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 2016, pp. 280–286.

[239] D. Jeske and P. van Schaik, "Familiarity with Internet threats: Beyond awareness," *Comput. Secur.*, vol. 66, pp. 129–141, May 2017.

[240] S. Taylor and P. A. Todd, "Understanding Information Technology Usage: A Test of Competing Models," *Inf. Syst. Res.*, vol. 6, no. 2, pp. 144–176, Jun. 1995.

[241] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Q.*, vol. 34, pp. 613–643, 2010.

[242] J. F. Hair Jr, G. T. Hult, C. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publishers, 2016.

[243] C. M. Ringle, D. Smith, and R. Reams, "Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers," *J. Fam. Bus. Strateg.*, vol. 5, no. 1, pp. 105–115, Mar. 2014.

[244] P. B. Lowry and J. Gaskin, "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It," *IEEE Trans. Prof. Commun.*, vol. 57, no. 2, pp. 123–146, Jun. 2014.

[245] S. Petter, D. Straub, and A. Rai, "Specifying Formative Constructs in Information Systems Research," *MIS Q.*, vol. 31, no. 4, p. 623, 2007.

[246] W. W. Chin, "The partial least squares approach to structural equation modeling," in *Modern methods for business research*, George A. Marcoulides, Ed. 1998, pp. 295–336.

[247] C. B. Jarvis, S. B. MacKenzie, and P. M. Podsakoff, "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *J. Consum. Res.*, vol. 30, no. 2, pp. 199–218, Sep. 2003.

[248] N. Ameen, R. Willis, and M. Hussain Shah, "An examination of the gender gap in smartphone adoption and use in Arab countries: A cross-national study," *Comput. Human Behav.*, vol. 89, pp. 148–162, Dec. 2018.

[249] I. Huvila and F. Ahmad, "Holistic information behavior and the perceived success of work in organizations," *Libr. Inf. Sci. Res.*, vol. 40, no. 1, pp. 18–29, Jan. 2018.

[250] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham, *Multivariate data analysis*, 7th ed. Prentice Hall, Upper Saddle River, NJ, 2010.

[251] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Mark. Sci.*, vol. 43, no. 1, pp. 115–135, Jan. 2015.

[252] J. Henseler, C. M. Ringle, and R. R. Sinkovics, "New Challenges to International Marketing The use of partial least squares path modeling in international marketing," *New Challenges to Int. Mark.*, pp. 277–319, 2015.

[253] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models

with Unobservable Variables and Measurement Error," *J. Mark. Res.*, vol. 18, no. 1, p. 39, Feb. 1981.

[254] P. A. Grassi *et al.*, "NIST Special Publication 800-63B, Digital Identity Guidelines," Gaithersburg, MD, Jun. 2019.

[255] G. D. Zimet, N. W. Dahlem, S. G. Zimet, and G. K. Farley, "The Multidimensional scale of perceived social support," *Artic. J. Personal. Assess.*, vol. 52, no. 1, pp. 30–41, 1988.

[256] J. E. Hupcey, "Clarifying the social support theory-research linkage," *J. Adv. Nurs.*, vol. 27, pp. 1231–1241, 1998.

Appendix A

Questionnaire used for Assessing Information Security Awareness among University Students – Chapter 3

The purpose of this study is to assess information security awareness (ISA) of the students and find relationship of different factors and ISA.

There are four sections in this questionnaire; Demographic information, General questions, Knowledge testing and Behavior testing. None of your personal information has been asked for and it has been tried that your identity is not disclosed in any way. The survey will take 10-15 minutes in total.

Thanking you for your time and interest in filling the questionnaire and your cooperation in this regard will be highly appreciated.

Regards, Ali Farooq (alifar@utu.fi)
Dept. of Future Technologies,
University of Turku, Finland.

Section I. Demographic Information

1. Gender M/F
2. Age
   Under 21 21-25 26-30 31-40 41-50 Above50
3. Current Study Level (Select one)
   - Undergraduate (Bachelor)
   - Graduate (Masters)
   - Post Graduate(PhD)
4. Field of studies (Select one)
   - Business Studies
   - Humanities
   - Law
   - Other Natural Science
   - Education
   - IT
   - Medicine/Medical Sciences
   - Social Sciences

5. Students background (Select one)
    - Local (Finnish origin/national)
    - International, please specify the country__________
6. How would you categorize the place, where you were living before coming to University of Turku? (Select one)
    - Rural (Small/median Town)
    - Urban (big town/small city)
    - Metropolitan (Big City)

Section II. General Questions

1. How do you rate your level of competency in IT?

   1(very low) 2(low) 3(Average) 4(high)
   5(very high) 6(unsure)

2. What is your perceived level of Information Security knowledge?

   1(very low) 2(low) 3(Average) 4(high)
   5(very high) 6(unsure)

3. Have you participated in some sort of training regarding Information Security.? Y/N

3a. If answer to previous question is YES, what was the nature of the training:
- Degree obligatory course(s)
- Non degree obligatory course(s)/Workshop(s)
- Voluntarily take course/workshop(s)

4. Do you have any work experience relevant to your field of study: Y/N

4a. If YES, type of work
- Part time
- Fulltime

4b. Duration of work experience:
- Less than 3 years
- 3-5 years
- More than 5 years

5. What is your source of information security knowledge, if any (Select all applicable)?
- Websites & search engines
- Journals
- Books
- Newspapers/Magazines

- Informal discussion with colleagues and professional contacts
- Formal Trainings (workshops, degree or non-degree courses)
- Others, specify _____________

6. What is your preferred source of information security knowledge? (Select one)

- Websites & search engines
- Journals
- Books
- Newspapers/Magazines
- Informal discussion with colleagues and professional contacts
- Formal Trainings (workshops, degree or non-degree courses)
- Others, specify _____________

Section III. Knowledge Testing

Read the following items and select the correct option as per your knowledge:

1. Worm is:

a. a computer program that replicates itself and spreads across a network
b. dependent upon security failures on the target computer in order to access it
c. created or designed only to spread and don't attempt to change the systems they pass through.
d. All of above
e. I do not know what does it mean?
f. I did not understand the alternatives well enough because of the language

2. Trojan Horse is:

a. a tale from Trojan wars in which a wooden horse was used to transfer soldiers into city of Troy
b. a program that pretends to be legitimate but contains some harmful program inside which gives access to target computer to a remote malicious party
c. a special breed of horse raised in England
d. All of above

e. I do not know what does it mean?
f. I did not understand the alternatives well enough because of the language

3. Spam is:
   a. Another word for e-mail or electronic messages
   b. A marketing technique
   c. Any unsolicited electronic mail
   d. All of above
   e. I do not know what spam is
4. Social Engineering is:
   a. influencing society on a large scale
   b. obtaining confidential information by manipulating and/or deceiving people
   c. a new type of society building measures
   d. All of above
   e. I do not know the term social engineering
   f. I did not understand the alternatives well enough because of the language
5. Phishing is:
   a. The use of an email message, that appears, to be legitimate, to solicit personal details
   b. Part of social engineering which means that someone is persuaded to give away confidential information
   c. Also referred to as identity theft
   d. All of the above
   e. I do not know what the term phishing means
   f. I did not understand the alternatives well enough because of the language
6. Pharming is:
   a. a hacker's attack that redirects a website's traffic to a bogus site without knowledge of the user
   b. phishing without a lure (trap)
   c. Both of above
   d. a technique used to create genetically modified organisms
   e. I do not know the term pharming
   f. I did not understand the alternatives well enough because of the language
7. Botnets are
   a. Used for click frauds
   b. Collection of computers connected through

Internet, whose control is ceded by a malicious party that can use these computers without knowledge and consent of the owners of those computers.

c. Often used for DDoS (Distributed Denial of Service) attacks
d. All of above
e. I do not know, what Botnet means
f. I did not understand the alternatives well enough because of the language

8. Denial of Service (DOS) attack is:

a. to flood the target with bogus requests preventing it to provide services to legitimate requests.
b. an incident in which user or organization is deprived of the services of a resource they would normally expect to have.
c. All of above
d. Related to disk operating system attacks
e. I do not understand this term
f. I did not understand the alternatives well enough because of the language

9. Zero day attack is:

a. an exploit in which someone takes advantage of a security vulnerability on the same day on which that vulnerability is detected
b. an attack that never has happened
c. an attack which is tried on an application the day it is released
d. all of above
e. I do not know this term
f. I did not understand the alternatives well enough because of the language

10. Security incident is:

a. A type of viral attack that is transferred from person to person working in a closed environment
b. An activity that may result in misuse, damage, denial of service, compromise of confidentiality of a network, computer, application, data.
c. An attack where a burglar breaks into a building
d. none of above

e. I do not know the term Security Incident

f. I did not understand the alternatives well enough because of the language

Section IV. Behavioral Questions

Read the following items and select the options that best describe you:

1. When receiving an e-mail that appears to be coming from your bank and asking you to go to a specific web link to confirm your personal details, what would you do? (select ALL that apply):

   a) If the bank's logo, address and all other information on the e-mail and webpage are correct, I will provide the required information.

   b) I will simply ignore the request.

   c) If my colleagues received the same request and if they have provided their details, I will do the same.

   d) I will phone the bank to find out about the request.

   e) I will report it to our company's IT department.

2. In case of any security incident, I will report to(specify):

____

3. You received an email with subject "You have won iPhone 5", what would you do? (Select ALL that apply):

   a) I will open the email and click on the link to see more information about the offer

   b) I will not open the email but simply delete it

   c) I will mark this email a "SPAM" in my email account without reading it

   d) I will open the email and will try to find the link from where I can unsubscribe my email to avoid any such email in future.

   e) I will open the email and analyze the content (sender email ID etc.) first.

4. Which of the following information you have shared online (on social networking sites or any other public space) (Select ALL that apply):

- Real Name,
- Email
- Real date of birth,
- Photographs of yourself,
- Photographs of your family,

- Full address,
- Phone number,
- Special occasions,
- Places you go to
- Photographs of your friends,
- Photographs of your office,
- Photographs of your home
- None of above

5. Which of the following information related to you, have ever been sent by you through email to anyone?(Select all that applies)
   - Social Security Number (SSN)
   - Credit Card Number
   - Login and/or password of online banking accoun
   - Bank Account Number
   - Pin Code of your Credit Card
   - Medical Data

6. Which of the following information related to you, have been sent to you through email? (Select all that applies)
   - Social Security Number (SSN)
   - Credit Card Number
   - Login and/or password of online banking account
   - Bank Account Number
   - Pin Code of your Credit Card
   - Medical Data

7. In terms of a new password, how do you store your password if you don’t want to forget it? (Select one)

   a) I will simply write it down somewhere
   b) I write down a hint/reminder for the password somewhere
   c) I write password/hint in a secure/locked place
   d) I memorize it
   e) I use password management tools.

8. Once a password is allotted for your universities email account, you do the following: (Select One most suitable)

   a) I never change my default password
   b) I change it when system asks me to change it
   c) I usually change it
   d) I always change it

9. How often do you change your passwords (select the one most appropriate):

a) Never
b) Rarely
c) Every 3 months
d) Every month
e) Whenever system prompts me to change it.

10. If requested whom you will disclose your password to:

a) Co-worker
b) Network Administrator
c) Head of Department
d) Supervisor
e) None of above

Appendix B

Items used for Studying Relationship of Information Security Awareness and Security Behaviour– Chapter 6

IMB Model Construct:	**Information**
Measure used	Threat Awareness (self-developed) (list of threats taken from [238], [239])
How would you rate your awareness to following threats to your information security and privacy? 1: Very poor to 5: Excellent	
TA1	Virus
TA2	Trojan
TA3	Malware
TA4	Rogueware/Ransomware
TA5	Botnet
TA6	Keylogger
TA7	Zero-day attack
TA8	Social engineering
TA9	e-mail harvesting
TA10	Spyware
TA11	virtual stalking
TA12	identify theft
TA13	internet surveillance (governmental/agencies)
TA14	Phishing
TA15	Cookies
TA16	Shoulder surfing
TA17	Data harvesting (Applications/apps)
TA18	Theft/loss of devices (laptops, tabs, phones)
TA19	Theft/loss of cards & wallets
TA20	Information Leakage-Online social networks

IMB Model Construct:	**Motivation/Personal**
Measure used	Security Attitude (adapted from [240])
Please read each of the following statement and select the option that best describes you (1: Strongly Disagree to 7: Strongly Agree)	
SA1	Using measures for information security is a good idea.
SA2*	Using measures for information security is foolish.
SA3*	I do not like using different security measures for my information security.
SA4	Using information security measures are for my benefit.
IMB Model Construct:	**Motivation/Social**
Measure used	Social Norm(adapted from [255], [256])
Please read each of the following statement and select the option that best describes you (1: Strongly Disagree to 7: Strongly Agree)	
SN1	Friends who influence my behavior think that I should take measures to for my information security
SN2	Significant others who are important to me think that I should take measures for my information security
SN3	My peers think that I should take security measures
IMB Model Construct:	**Behavioral Skills**
Measure used	Self-efficacy (adapted from [172], [240])
Please read each of the following statement and select the option that best describes you (1: Strongly Disagree to 7: Strongly Agree)	
SE1	I feel comfortable taking measures to secure my information security.
SE2	Taking the necessary security measures is entirely under my control.
SE3	I have the resources and the knowledge to take the necessary security measures.
SE4	Taking the necessary security measures is easy.
SE5	I can protect my information security by myself.
SE6	I can enable security measures on my system (computer/laptop).

IMB Model Construct:	**Behavioral Skills**
Measure used	Measures Familiarity (list of measures taken from [227])
How would you rate your familiarity with the following security measures? *(1: Not at all familiar to 5: Extremely familiar)*	
MF1	Use of anti-virus software
MF2	Automatic Operating System (OS) updates
MF3	Update anti-virus software regularly
MF4	Use software from trusted sources
MF5	Change passwords regularly
MF6	Use of two-factor authentication
MF7	Use of strong passwords
MF8	Use of unique passwords
MF9	Use of password manager
MF10	Avoid clicking unexpected emails attachments
MF11	Not responding to emails from strangers
MF12	Taking your data backups regularly
MF13	Deleting cookies/Browsing history
MF14	Use of VPN
MF15	Check for HTTPS while browsing
MF16	Verify URL of the websites
MF17	Avoid clicking ads
MF18	Be critical and suspicious while surfing
MF19	Avoid sharing personal information online
MF20	Use of Linux
IMB Model Construct:	**Behavior**
Measure used	Security Behavior (list taken from [228])
Please read each of the following statement and select the option that best describes you *(1: Never, 2: Rarely, 3: Sometimes, 4: Often, 5: Always)*	
SB1	I verify that my anti-virus software has been regularly updating itself
SB2	When I am prompted of about operating system update, I install it right away.
SB3	I use different passwords for different accounts.
SB4	When I create passwords for my accounts, I include alpha-numeric characters (for example, A, a, *, %,1) so that it is not easy to guess.

SB5	I install software updates right away when prompted.
SB6	I use password management tools (password managers) for better password management and protection.
SB7	While sending or entering personal information on a website I first make sure that the website is secure by checking "https:// or lock sign".
SB8	I download software/applications from trusted sources only.
SB9	I use two-factor authentication, where available.
SB10*	While web-surfing, I get rid of appearing dialogue boxes quickly by clicking "OK", without reading the message, so that I continue with my surfing.
SB11	I manually lock my computer screen when I step away from it.
SB12	I avoid opening attachments that I am not expecting.

** items reverse coded for analysis*

Turku Centre for Computer Science
TUCS Dissertations

1. **Marjo Lipponen**, On Primitive Solutions of the Post Correspondence Problem
2. **Timo Käkölä**, Dual Information Systems in Hyperknowledge Organizations
3. **Ville Leppänen**, Studies on the Realization of PRAM
4. **Cunsheng Ding**, Cryptographic Counter Generators
5. **Sami Viitanen**, Some New Global Optimization Algorithms
6. **Tapio Salakoski**, Representative Classification of Protein Structures
7. **Thomas Långbacka**, An Interactive Environment Supporting the Development of Formally Correct Programs
8. **Thomas Finne**, A Decision Support System for Improving Information Security
9. **Valeria Mihalache**, Cooperation, Communication, Control. Investigations on Grammar Systems.
10. **Marina Waldén**, Formal Reasoning About Distributed Algorithms
11. **Tero Laihonen**, Estimates on the Covering Radius When the Dual Distance is Known
12. **Lucian Ilie**, Decision Problems on Orders of Words
13. **Jukkapekka Hekanaho**, An Evolutionary Approach to Concept Learning
14. **Jouni Järvinen**, Knowledge Representation and Rough Sets
15. **Tomi Pasanen**, In-Place Algorithms for Sorting Problems
16. **Mika Johnsson**, Operational and Tactical Level Optimization in Printed Circuit Board Assembly
17. **Mats Aspnäs**, Multiprocessor Architecture and Programming: The Hathi-2 System
18. **Anna Mikhajlova**, Ensuring Correctness of Object and Component Systems
19. **Vesa Torvinen**, Construction and Evaluation of the Labour Game Method
20. **Jorma Boberg**, Cluster Analysis. A Mathematical Approach with Applications to Protein Structures
21. **Leonid Mikhajlov**, Software Reuse Mechanisms and Techniques: Safety Versus Flexibility
22. **Timo Kaukoranta**, Iterative and Hierarchical Methods for Codebook Generation in Vector Quantization
23. **Gábor Magyar**, On Solution Approaches for Some Industrially Motivated Combinatorial Optimization Problems
24. **Linas Laibinis**, Mechanised Formal Reasoning About Modular Programs
25. **Shuhua Liu**, Improving Executive Support in Strategic Scanning with Software Agent Systems
26. **Jaakko Järvi**, New Techniques in Generic Programming – C++ is more Intentional than Intended
27. **Jan-Christian Lehtinen**, Reproducing Kernel Splines in the Analysis of Medical Data
28. **Martin Büchi**, Safe Language Mechanisms for Modularization and Concurrency
29. **Elena Troubitsyna**, Stepwise Development of Dependable Systems
30. **Janne Näppi**, Computer-Assisted Diagnosis of Breast Calcifications
31. **Jianming Liang**, Dynamic Chest Images Analysis
32. **Tiberiu Seceleanu**, Systematic Design of Synchronous Digital Circuits
33. **Tero Aittokallio**, Characterization and Modelling of the Cardiorespiratory System in Sleep-Disordered Breathing
34. **Ivan Porres**, Modeling and Analyzing Software Behavior in UML
35. **Mauno Rönkkö**, Stepwise Development of Hybrid Systems
36. **Jouni Smed**, Production Planning in Printed Circuit Board Assembly
37. **Vesa Halava**, The Post Correspondence Problem for Market Morphisms
38. **Ion Petre**, Commutation Problems on Sets of Words and Formal Power Series
39. **Vladimir Kvassov**, Information Technology and the Productivity of Managerial Work
40. **Frank Tétard**, Managers, Fragmentation of Working Time, and Information Systems

41. **Jan Manuch**, Defect Theorems and Infinite Words
42. **Kalle Ranto**, Z_4-Goethals Codes, Decoding and Designs
43. **Arto Lepistö**, On Relations Between Local and Global Periodicity
44. **Mika Hirvensalo**, Studies on Boolean Functions Related to Quantum Computing
45. **Pentti Virtanen**, Measuring and Improving Component-Based Software Development
46. **Adekunle Okunoye**, Knowledge Management and Global Diversity – A Framework to Support Organisations in Developing Countries
47. **Antonina Kloptchenko**, Text Mining Based on the Prototype Matching Method
48. **Juha Kivijärvi**, Optimization Methods for Clustering
49. **Rimvydas Rukšėnas**, Formal Development of Concurrent Components
50. **Dirk Nowotka**, Periodicity and Unbordered Factors of Words
51. **Attila Gyenesei**, Discovering Frequent Fuzzy Patterns in Relations of Quantitative Attributes
52. **Petteri Kaitovaara**, Packaging of IT Services – Conceptual and Empirical Studies
53. **Petri Rosendahl**, Niho Type Cross-Correlation Functions and Related Equations
54. **Péter Majlender**, A Normative Approach to Possibility Theory and Soft Decision Support
55. **Seppo Virtanen**, A Framework for Rapid Design and Evaluation of Protocol Processors
56. **Tomas Eklund**, The Self-Organizing Map in Financial Benchmarking
57. **Mikael Collan**, Giga-Investments: Modelling the Valuation of Very Large Industrial Real Investments
58. **Dag Björklund**, A Kernel Language for Unified Code Synthesis
59. **Shengnan Han**, Understanding User Adoption of Mobile Technology: Focusing on Physicians in Finland
60. **Irina Georgescu**, Rational Choice and Revealed Preference: A Fuzzy Approach
61. **Ping Yan**, Limit Cycles for Generalized Liénard-Type and Lotka-Volterra Systems
62. **Joonas Lehtinen**, Coding of Wavelet-Transformed Images
63. **Tommi Meskanen,** On the NTRU Cryptosystem
64. **Saeed Salehi**, Varieties of Tree Languages
65. **Jukka Arvo**, Efficient Algorithms for Hardware-Accelerated Shadow Computation
66. **Mika Hirvikorpi**, On the Tactical Level Production Planning in Flexible Manufacturing Systems
67. **Adrian Costea**, Computational Intelligence Methods for Quantitative Data Mining
68. **Cristina Seceleanu**, A Methodology for Constructing Correct Reactive Systems
69. **Luigia Petre**, Modeling with Action Systems
70. **Lu Yan**, Systematic Design of Ubiquitous Systems
71. **Mehran Gomari**, On the Generalization Ability of Bayesian Neural Networks
72. **Ville Harkke**, Knowledge Freedom for Medical Professionals – An Evaluation Study of a Mobile Information System for Physicians in Finland
73. **Marius Cosmin Codrea**, Pattern Analysis of Chlorophyll Fluorescence Signals
74. **Aiying Rong**, Cogeneration Planning Under the Deregulated Power Market and Emissions Trading Scheme
75. **Chihab BenMoussa**, Supporting the Sales Force through Mobile Information and Communication Technologies: Focusing on the Pharmaceutical Sales Force
76. **Jussi Salmi**, Improving Data Analysis in Proteomics
77. **Orieta Celiku**, Mechanized Reasoning for Dually-Nondeterministic and Probabilistic Programs
78. **Kaj-Mikael Björk**, Supply Chain Efficiency with Some Forest Industry Improvements
79. **Viorel Preoteasa**, Program Variables – The Core of Mechanical Reasoning about Imperative Programs
80. **Jonne Poikonen**, Absolute Value Extraction and Order Statistic Filtering for a Mixed-Mode Array Image Processor
81. **Luka Milovanov**, Agile Software Development in an Academic Environment
82. **Francisco Augusto Alcaraz Garcia**, Real Options, Default Risk and Soft Applications
83. **Kai K. Kimppa**, Problems with the Justification of Intellectual Property Rights in Relation to Software and Other Digitally Distributable Media
84. **Dragoş Truşcan**, Model Driven Development of Programmable Architectures
85. **Eugen Czeizler**, The Inverse Neighborhood Problem and Applications of Welch Sets in Automata Theory

86. **Sanna Ranto**, Identifying and Locating-Dominating Codes in Binary Hamming Spaces
87. **Tuomas Hakkarainen**, On the Computation of the Class Numbers of Real Abelian Fields
88. **Elena Czeizler**, Intricacies of Word Equations
89. **Marcus Alanen**, A Metamodeling Framework for Software Engineering
90. **Filip Ginter**, Towards Information Extraction in the Biomedical Domain: Methods and Resources
91. **Jarkko Paavola**, Signature Ensembles and Receiver Structures for Oversaturated Synchronous DS-CDMA Systems
92. **Arho Virkki**, The Human Respiratory System: Modelling, Analysis and Control
93. **Olli Luoma**, Efficient Methods for Storing and Querying XML Data with Relational Databases
94. **Dubravka Ilić**, Formal Reasoning about Dependability in Model-Driven Development
95. **Kim Solin**, Abstract Algebra of Program Refinement
96. **Tomi Westerlund**, Time Aware Modelling and Analysis of Systems-on-Chip
97. **Kalle Saari**, On the Frequency and Periodicity of Infinite Words
98. **Tomi Kärki**, Similarity Relations on Words: Relational Codes and Periods
99. **Markus M. Mäkelä**, Essays on Software Product Development: A Strategic Management Viewpoint
100. **Roope Vehkalahti**, Class Field Theoretic Methods in the Design of Lattice Signal Constellations
101. **Anne-Maria Ernvall-Hytönen**, On Short Exponential Sums Involving Fourier Coefficients of Holomorphic Cusp Forms
102. **Chang Li**, Parallelism and Complexity in Gene Assembly
103. **Tapio Pahikkala**, New Kernel Functions and Learning Methods for Text and Data Mining
104. **Denis Shestakov**, Search Interfaces on the Web: Querying and Characterizing
105. **Sampo Pyysalo**, A Dependency Parsing Approach to Biomedical Text Mining
106. **Anna Sell**, Mobile Digital Calendars in Knowledge Work
107. **Dorina Marghescu**, Evaluating Multidimensional Visualization Techniques in Data Mining Tasks
108. **Tero Säntti**, A Co-Processor Approach for Efficient Java Execution in Embedded Systems
109. **Kari Salonen**, Setup Optimization in High-Mix Surface Mount PCB Assembly
110. **Pontus Boström**, Formal Design and Verification of Systems Using Domain-Specific Languages
111. **Camilla J. Hollanti**, Order-Theoretic Mehtods for Space-Time Coding: Symmetric and Asymmetric Designs
112. **Heidi Himmanen**, On Transmission System Design for Wireless Broadcasting
113. **Sébastien Lafond**, Simulation of Embedded Systems for Energy Consumption Estimation
114. **Evgeni Tsivtsivadze**, Learning Preferences with Kernel-Based Methods
115. **Petri Salmela**, On Commutation and Conjugacy of Rational Languages and the Fixed Point Method
116. **Siamak Taati**, Conservation Laws in Cellular Automata
117. **Vladimir Rogojin**, Gene Assembly in Stichotrichous Ciliates: Elementary Operations, Parallelism and Computation
118. **Alexey Dudkov**, Chip and Signature Interleaving in DS CDMA Systems
119. **Janne Savela**, Role of Selected Spectral Attributes in the Perception of Synthetic Vowels
120. **Kristian Nybom**, Low-Density Parity-Check Codes for Wireless Datacast Networks
121. **Johanna Tuominen**, Formal Power Analysis of Systems-on-Chip
122. **Teijo Lehtonen**, On Fault Tolerance Methods for Networks-on-Chip
123. **Eeva Suvitie**, On Inner Products Involving Holomorphic Cusp Forms and Maass Forms
124. **Linda Mannila**, Teaching Mathematics and Programming – New Approaches with Empirical Evaluation
125. **Hanna Suominen**, Machine Learning and Clinical Text: Supporting Health Information Flow
126. **Tuomo Saarni**, Segmental Durations of Speech
127. **Johannes Eriksson**, Tool-Supported Invariant-Based Programming

128. **Tero Jokela**, Design and Analysis of Forward Error Control Coding and Signaling for Guaranteeing QoS in Wireless Broadcast Systems
129. **Ville Lukkarila**, On Undecidable Dynamical Properties of Reversible One-Dimensional Cellular Automata
130. **Qaisar Ahmad Malik**, Combining Model-Based Testing and Stepwise Formal Development
131. **Mikko-Jussi Laakso**, Promoting Programming Learning: Engagement, Automatic Assessment with Immediate Feedback in Visualizations
132. **Riikka Vuokko**, A Practice Perspective on Organizational Implementation of Information Technology
133. **Jeanette Heidenberg**, Towards Increased Productivity and Quality in Software Development Using Agile, Lean and Collaborative Approaches
134. **Yong Liu**, Solving the Puzzle of Mobile Learning Adoption
135. **Stina Ojala**, Towards an Integrative Information Society: Studies on Individuality in Speech and Sign
136. **Matteo Brunelli**, Some Advances in Mathematical Models for Preference Relations
137. **Ville Junnila**, On Identifying and Locating-Dominating Codes
138. **Andrzej Mizera**, Methods for Construction and Analysis of Computational Models in Systems Biology. Applications to the Modelling of the Heat Shock Response and the Self-Assembly of Intermediate Filaments.
139. **Csaba Ráduly-Baka**, Algorithmic Solutions for Combinatorial Problems in Resource Management of Manufacturing Environments
140. **Jari Kyngäs**, Solving Challenging Real-World Scheduling Problems
141. **Arho Suominen**, Notes on Emerging Technologies
142. **József Mezei**, A Quantitative View on Fuzzy Numbers
143. **Marta Olszewska**, On the Impact of Rigorous Approaches on the Quality of Development
144. **Antti Airola**, Kernel-Based Ranking: Methods for Learning and Performace Estimation
145. **Aleksi Saarela**, Word Equations and Related Topics: Independence, Decidability and Characterizations
146. **Lasse Bergroth**, Kahden merkkijonon pisimmän yhteisen alijonon ongelma ja sen ratkaiseminen
147. **Thomas Canhao Xu**, Hardware/Software Co-Design for Multicore Architectures
148. **Tuomas Mäkilä**, Software Development Process Modeling – Developers Perspective to Contemporary Modeling Techniques
149. **Shahrokh Nikou**, Opening the Black-Box of IT Artifacts: Looking into Mobile Service Characteristics and Individual Perception
150. **Alessandro Buoni**, Fraud Detection in the Banking Sector: A Multi-Agent Approach
151. **Mats Neovius**, Trustworthy Context Dependency in Ubiquitous Systems
152. **Fredrik Degerlund**, Scheduling of Guarded Command Based Models
153. **Amir-Mohammad Rahmani-Sane**, Exploration and Design of Power-Efficient Networked Many-Core Systems
154. **Ville Rantala**, On Dynamic Monitoring Methods for Networks-on-Chip
155. **Mikko Pelto**, On Identifying and Locating-Dominating Codes in the Infinite King Grid
156. **Anton Tarasyuk**, Formal Development and Quantitative Verification of Dependable Systems
157. **Muhammad Mohsin Saleemi**, Towards Combining Interactive Mobile TV and Smart Spaces: Architectures, Tools and Application Development
158. **Tommi J. M. Lehtinen**, Numbers and Languages
159. **Peter Sarlin**, Mapping Financial Stability
160. **Alexander Wei Yin**, On Energy Efficient Computing Platforms
161. **Mikołaj Olszewski**, Scaling Up Stepwise Feature Introduction to Construction of Large Software Systems
162. **Maryam Kamali**, Reusable Formal Architectures for Networked Systems
163. **Zhiyuan Yao**, Visual Customer Segmentation and Behavior Analysis – A SOM-Based Approach
164. **Timo Jolivet**, Combinatorics of Pisot Substitutions
165. **Rajeev Kumar Kanth**, Analysis and Life Cycle Assessment of Printed Antennas for Sustainable Wireless Systems
166. **Khalid Latif**, Design Space Exploration for MPSoC Architectures

167. **Bo Yang**, Towards Optimal Application Mapping for Energy-Efficient Many-Core Platforms
168. **Ali Hanzala Khan**, Consistency of UML Based Designs Using Ontology Reasoners
169. **Sonja Leskinen**, m-Equine: IS Support for the Horse Industry
170. **Fareed Ahmed Jokhio**, Video Transcoding in a Distributed Cloud Computing Environment
171. **Moazzam Fareed Niazi**, A Model-Based Development and Verification Framework for Distributed System-on-Chip Architecture
172. **Mari Huova**, Combinatorics on Words: New Aspects on Avoidability, Defect Effect, Equations and Palindromes
173. **Ville Timonen**, Scalable Algorithms for Height Field Illumination
174. **Henri Korvela**, Virtual Communities – A Virtual Treasure Trove for End-User Developers
175. **Kameswar Rao Vaddina**, Thermal-Aware Networked Many-Core Systems
176. **Janne Lahtiranta**, New and Emerging Challenges of the ICT-Mediated Health and Well-Being Services
177. **Irum Rauf**, Design and Validation of Stateful Composite RESTful Web Services
178. **Jari Björne**, Biomedical Event Extraction with Machine Learning
179. **Katri Haverinen**, Natural Language Processing Resources for Finnish: Corpus Development in the General and Clinical Domains
180. **Ville Salo**, Subshifts with Simple Cellular Automata
181. **Johan Ersfolk**, Scheduling Dynamic Dataflow Graphs
182. **Hongyan Liu**, On Advancing Business Intelligence in the Electricity Retail Market
183. **Adnan Ashraf**, Cost-Efficient Virtual Machine Management: Provisioning, Admission Control, and Consolidation
184. **Muhammad Nazrul Islam**, Design and Evaluation of Web Interface Signs to Improve Web Usability: A Semiotic Framework
185. **Johannes Tuikkala**, Algorithmic Techniques in Gene Expression Processing: From Imputation to Visualization
186. **Natalia Díaz Rodríguez**, Semantic and Fuzzy Modelling for Human Behaviour Recognition in Smart Spaces. A Case Study on Ambient Assisted Living
187. **Mikko Pänkäälä**, Potential and Challenges of Analog Reconfigurable Computation in Modern and Future CMOS
188. **Sami Hyrynsalmi**, Letters from the War of Ecosystems – An Analysis of Independent Software Vendors in Mobile Application Marketplaces
189. **Seppo Pulkkinen**, Efficient Optimization Algorithms for Nonlinear Data Analysis
190. **Sami Pyöttiälä**, Optimization and Measuring Techniques for Collect-and-Place Machines in Printed Circuit Board Industry
191. **Syed Mohammad Asad Hassan Jafri**, Virtual Runtime Application Partitions for Resource Management in Massively Parallel Architectures
192. **Toni Ernvall**, On Distributed Storage Codes
193. **Yuliya Prokhorova**, Rigorous Development of Safety-Critical Systems
194. **Olli Lahdenoja**, Local Binary Patterns in Focal-Plane Processing – Analysis and Applications
195. **Annika H. Holmbom**, Visual Analytics for Behavioral and Niche Market Segmentation
196. **Sergey Ostroumov**, Agent-Based Management System for Many-Core Platforms: Rigorous Design and Efficient Implementation
197. **Espen Suenson**, How Computer Programmers Work – Understanding Software Development in Practise
198. **Tuomas Poikela**, Readout Architectures for Hybrid Pixel Detector Readout Chips
199. **Bogdan Iancu**, Quantitative Refinement of Reaction-Based Biomodels
200. **Ilkka Törmä**, Structural and Computational Existence Results for Multidimensional Subshifts
201. **Sebastian Okser**, Scalable Feature Selection Applications for Genome-Wide Association Studies of Complex Diseases
202. **Fredrik Abbors**, Model-Based Testing of Software Systems: Functionality and Performance
203. **Inna Pereverzeva**, Formal Development of Resilient Distributed Systems
204. **Mikhail Barash**, Defining Contexts in Context-Free Grammars
205. **Sepinoud Azimi**, Computational Models for and from Biology: Simple Gene Assembly and Reaction Systems
206. **Petter Sandvik**, Formal Modelling for Digital Media Distribution

207. **Jongyun Moon**, Hydrogen Sensor Application of Anodic Titanium Oxide Nanostructures
208. **Simon Holmbacka**, Energy Aware Software for Many-Core Systems
209. **Charalampos Zinoviadis**, Hierarchy and Expansiveness in Two-Dimensional Subshifts of Finite Type
210. **Mika Murtojärvi**, Efficient Algorithms for Coastal Geographic Problems
211. **Sami Mäkelä**, Cohesion Metrics for Improving Software Quality
212. **Eyal Eshet**, Examining Human-Centered Design Practice in the Mobile Apps Era
213. **Jetro Vesti**, Rich Words and Balanced Words
214. **Jarkko Peltomäki**, Privileged Words and Sturmian Words
215. **Fahimeh Farahnakian**, Energy and Performance Management of Virtual Machines: Provisioning, Placement and Consolidation
216. **Diana-Elena Gratie**, Refinement of Biomodels Using Petri Nets
217. **Harri Merisaari**, Algorithmic Analysis Techniques for Molecular Imaging
218. **Stefan Grönroos**, Efficient and Low-Cost Software Defined Radio on Commodity Hardware
219. **Noora Nieminen**, Garbling Schemes and Applications
220. **Ville Taajamaa**, O-CDIO: Engineering Education Framework with Embedded Design Thinking Methods
221. **Johannes Holvitie**, Technical Debt in Software Development – Examining Premises and Overcoming Implementation for Efficient Management
222. **Tewodros Deneke**, Proactive Management of Video Transcoding Services
223. **Kashif Javed**, Model-Driven Development and Verification of Fault Tolerant Systems
224. **Pekka Naula**, Sparse Predictive Modeling – A Cost-Effective Perspective
225. **Antti Hakkala**, On Security and Privacy for Networked Information Society – Observations and Solutions for Security Engineering and Trust Building in Advanced Societal Processes
226. **Anne-Maarit Majanoja**, Selective Outsourcing in Global IT Services – Operational Level Challenges and Opportunities
227. **Samuel Rönnqvist**, Knowledge-Lean Text Mining
228. **Mohammad-Hashem Hahgbayan**, Energy-Efficient and Reliable Computing in Dark Silicon Era
229. **Charmi Panchal**, Qualitative Methods for Modeling Biochemical Systems and Datasets: The Logicome and the Reaction Systems Approaches
230. **Erkki Kaila**, Utilizing Educational Technology in Computer Science and Programming Courses: Theory and Practice
231. **Fredrik Robertsén**, The Lattice Boltzmann Method, a Petaflop and Beyond
232. **Jonne Pohjankukka**, Machine Learning Approaches for Natural Resource Data
233. **Paavo Nevalainen**, Geometric Data Understanding: Deriving Case-Specific Features
234. **Michal Szabados**, An Algebraic Approach to Nivat's Conjecture
235. **Tuan Nguyen Gia**, Design for Energy-Efficient and Reliable Fog-Assisted Healthcare IoT Systems
236. **Anil Kanduri**, Adaptive Knobs for Resource Efficient Computing
237. **Veronika Suni**, Computational Methods and Tools for Protein Phosphorylation Analysis
238. **Behailu Negash**, Interoperating Networked Embedded Systems to Compose the Web of Things
239. **Kalle Rindell**, Development of Secure Software: Rationale, Standards and Practices
240. **Jurka Rahikkala**, On Top Management Support for Software Cost Estimation
241. **Markus A. Whiteland**, On the k-Abelian Equivalence Relation of Finite Words
242. **Mojgan Kamali**, Formal Analysis of Network Routing Protocols
243. **Jesús Carabaño Bravo**, A Compiler Approach to Map Algebra for Raster Spatial Modeling
244. **Amin Majd**, Distributed and Lightweight Meta-heuristic Optimization Method for Complex Problems
245. **Ali Farooq**, In Quest of Information Security in Higher Education Institutions: Security Awareness, Concerns, and Behaviour of Students

Turku
Centre *for*
Computer
Science

http://www.tucs.fi
tucs@abo.fi

University of Turku
Faculty of Mathematics and Natural Sciences
- Department of Future Technologies
- Department of Mathematics and Statistics

Turku School of Economics
- Institute of Information Systems Science

Åbo Akademi University
Faculty of Science and Engineering
- Computer Engineering
- Computer Science

Faculty of Social Sciences, Business and Economics
- Information Systems

ISBN 978-952-12-3879-6
ISSN 1239-1883

Ali Farooq

In Quest of Information Security in Higher Education Institutions

Ali Farooq

In Quest of Information Security in Higher Education Institutions

Ali Farooq

In Quest of Information Security in Higher Education Institutions