EVALUATION MODEL FOR KNOWLEDGE SHARING IN INFORMATION SECURITY PROFESSIONAL VIRTUAL COMMUNITY

ALIREZA TAMJIDYAMCHOLO

THESIS SUBMITTED AS FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA

2014

Abstract

Cyberspace communities can be considered as a warehouse of knowledge that provides people with an opportunity to receive or share information. The most important challenge for knowledge sharing among information security professionals is motivating participation in knowledge sharing. Many professional virtual communities (PVC) have failed due to reasons, such as the low willingness of members to share knowledge with others. This research proposes two models to evaluate and understand the determinants of knowledge sharing behavior in PVCs. In the first model, nine hypotheses have been examined while five hypotheses have been examined in the second model. First model analyses key factors, consist of attitude, self-efficacy, trust, norm of reciprocity, and shared language, with respect to the information security workers' intention to share knowledge. Information security professionals in virtual communities, including the Information Security Professional Association (ISPA), Information Systems Security Association (ISSA), Society of Information Risk Analysts (SIRA), and LinkedIn security groups, were surveyed to test the proposed model. Confirmatory factor analysis (CFA) and the structural equation modelling (SEM) technique were used to analyse the data and evaluate the research model. The results show that the research model fit the data well and the structural model suggests a strong relationship between attitude, trust, and norms of reciprocity to knowledge sharing intention. Hypotheses regarding the influence of self-efficacy and reciprocity, to knowledge sharing attitude were upheld. Shared language did not influence either the attitude or intention to share knowledge. The second model is composed of two main parts. The first part is the Triandis theory, which is adapted to analyse the other determinants of knowledge sharing behavior in PVCs. The second part explores the quantitative relationship between knowledge sharing and security risk reduction. One hundred and forty-two members from the LinkedIn information security groups

participated in this study. PLS analysis shows that perceived consequences, affect, and facilitating conditions have significant effects on knowledge sharing behavior. In contrast, social factors have shown insignificant effects on knowledge sharing behavior. The results of the study demonstrate that there is a positive and strong relationship between knowledge sharing behavior and information security risk reduction.

Abstrak

Komuniti ruang siber boleh dianggap sebagai satu gudang ilmu yang menawarkan peluang untuk orang ramai menerima dan berkongsi maklumat. Cabaran yang paling penting dalam perkongsian maklumat di antara ahli-ahli pakar sekuriti maklumat ialah memotivasikan penyertaan dalam perkongsian maklumat. Ramai komuniti pakar secara maya (PVC) gagal kerana kurangnya kemahuan ahli untuk berkongsi maklumat dengan orang lain. Kajian ini mencadangkan dua model untuk menilai dan memahami kesanggupan perkongsian maklumat dikalangan PVC. Di dalam model pertama, sembilan hipotesis telah dikaji manakala lima hipotesis dikaji dalam model kedua. Faktor utama model pertama merangkumi sikap, keberkesanan, kepercayaan, norma timbal balik dan juga perkongsian bahasa terhadap kesanggupan pekerja-pekerja keselamatan maklumat untuk berkongsi maklumat. Pakar-pakar keselamatan maklumat dalam komuniti alam maya, termasuk Persatuan Pakar Keselamatan Maklumat (ISPA), Persatuan Sistem Keselamatan Maklumat (ISSA), Persatuan Analisis Risiko Maklumat (SIRA) dan organisasi keselamatan LinkedIn telah dikaji untuk menguji model yang dicadangkan. Teknik analisis factor pengesahan (CFA) dan pemodelan persamaan struktural (SEM) telah digunakan untuk menganalisis data dan juga menilai model kajian. Hasil keputusan menunjukkan model kajian sesuai dengan data dengan baik dan model struktural mencadangkan bahawa wujud hubung kait yang kuat di antara sikap, kepercayaan dan norma timbal balik dengan niat perkongsian maklumat. Hipotesis mengenai pengaruh keberkesanan diri dan persalingan terhadap sikap perkongsian maklumat telah tercapai. Perkongsian bahasa tidak mempengaruhi sikap atau niat untuk perkongsian maklumat. Model kedua merangkumi dua bahagian. Bahagian pertama merangkumi teori Triandis yang diadaptasi untuk menganalisis penentu-penentu lain tingkah laku perkongsian maklumat dikalangan PVC. Bahagian kedua mengkaji hubung kait kuantitatif di antara perkongsian maklumat dan pengurangan

risiko keselamatan. Seratus empat puluh dua orang ahli dari organisasi sekuriti maklumat LinkedIn telah menyertai kajian ini. Analisis PLS menunjukkan kesan yang dapat dilihat, kesan penjejasan dan keadaan memudahkan, mempunyai kesan yang signifikan terhadap tingkah laku perkongsian maklumat. Sebaliknya, faktor-faktor sosial menunjukkan kesan yang tidak signifikan terhadap tingkah laku perkongsian maklumat. Keputusan kajian ini menunjukkan bahawa terdapat perhubungan positif dan kuat di antara tingkah laku perkongsian maklumat dan pengurangan risiko keselamatan maklumat.

Dedication

This is dedicated to my spouse for her never-ending love as well as support; to my parents who never lost faith in me; and to my brother and sisters who believed in me, and wished only for my success.

Acknowledgements

First and foremost, I offer my sincerest gratitude to Allah the Almighty for bestowing me with the opportunity and good health to complete my dissertation successfully. I would also like to thank my supervisors, Prof. Dr. Mohd Sapiyan Bin Baba, Assoc. Prof. Datin Dr. Sameem Abdul Kareem, and Dr. Nor Liyana Mohd Shuib for help, advice, and mentoring throughout my graduate career. Without their support and guidance, none of the work presented in this thesis would have been possible. Moreover, I am deeply indebted to them for showing me how to successfully do research, mentor students, and communicate the research results effectively.

April, 2014

Table of Contents

List of Figures

List of Tables

List of Abbreviations

CFA	:	Confirmatory Factor Analysis
InfoSec	:	Information Security
IS	:	Information System
ISM	:	Information Security Management
ISPA	:	Information Security Professional Association
ISRM	:	Information Security Risk Management
ISSA	:	Information Systems Security Association
IT-ISAC	:	Information Technology Information Sharing and Analysis Centre
IT	:	Information Technology
KM	:	Knowledge Management
KS	:	Knowledge Sharing
PLS	:	Partial Least Squares
PVC	:	Professional Virtual Community
SEM	:	Structural Equation Modelling
SIRA	:	Society of Information Risk Analysts
VC	:	Virtual Community

CHAPTER 1

INTRODUCTION

1.1 Research Background

Information technology has faced a serious issue in recent years pertaining to cyber-attacks and security breaches. A large and diverse number of institutions have been the targets of such attacks, ranging from high-profile firms to prestigious universities. Richardson (2011) in the fifteenth yearly computer crime and security study pointed out that 41% of participants had confirmed that they had experienced a security incident over the course of the year. According to Richardson (2011), this study had been performed in 351 industrial units with various backgrounds; namely, educational services, financial services, health services and manufacturing. Very few participants were inclined to give out the exact amount of financial losses. However, two respondents revealed their losses, which were sizably large; namely, $20 million in total for one and $25 million for another.

Nowadays, financial profits are the key motivation for hackers, while many people may think they look for personal information or for more excitement (Liu, Ji & Mookerjee, 2011). Hence, it is quite reasonable to see that organizations that depend on the Internet for their major business activities take serious precautions for information security (Szymanski & Hise, 2000; Chen, Schmidt, Phan & Arnett, 2008). Nonetheless, those institutions that are not directly dependent on the Internet for their business activities still regard information security as a vital issue. This is because such organizations have access to plenty of personal and sensitive information about their customers, product sales, and technical information. More funding in the information security sector is considered a major initiative for institutions to achieve more information security.

One of the initiatives that organizations can apply to increase information security is to invest in security technologies; namely, antivirus software, firewalls, sophisticated encryption technology, intrusion detection systems, and other hardware devices (Hamill, Deckro & Kloeber, 2005; Liu, Tanaka & Matsuura, 2006). The investment fund must be cautiously balanced with the effects they can create in information security. It is also possible for companies to enhance their information security via cooperating and sharing technical security information with other companies. It has been shown by a number of experimental studies that institutions can save their investment expenditure when they share their security knowledge with each other and that it can help them to decrease their expenses (Liu, Ji & Mookerjee, 2011; Gal-Or & Ghose, 2005; Gordon, Loeb & Lucyshyn, 2003). The Information Technology Information Sharing and Analysis Centre (IT-ISAC) (https://www.it-isac.org) can be viewed as a good example of security knowledge sharing. The major goal of this center is to assist in sharing information on cyber-security threats and vulnerabilities. An impartial forum is designed for members of this center to communicate with peers from other companies in order to share and identify technical and non-public details of threats and vulnerabilities. In addition, members can have access to a trusted point of contact for knowledge sharing before or during forum sessions.

Nowadays, IT security specialists attempt to maintain a strict security standard in information systems, but are baffled by similar problems in doing so, and need to find effective ways to circumvent such problems. However, when specialists have the chance to share their knowledge such situations would not arise as they would be able to provide high quality solutions and enhance previous approaches rather than just reinventing the security wheel. Currently, virtual space is a common and joint environment in which experts are able to find each other and share their knowledge and information (Lin, Lin & Huang, 2008). Research workers have mentioned that virtual

communities often fail in fostering knowledge sharing efforts because they are oblivious of the willingness of individuals to share knowledge and the knowledge that is needed for successful knowledge sharing (Chen & Hung, 2010; Lin, Hung & Chen, 2009) .

1.2 Problem Statement

The presence of virtual communities in information security field broadens and clusters individual online activities. The fundamental step of creating a virtual community is the provision of knowledge, which can be achieved through increasing participants' willingness to share knowledge and information with other users. Sharing of information and experience amid information security professionals significantly saves investment in information security (Liu, Ji & Mookerjee, 2011). Furthermore, sharing knowledge among information security technicians can restrain an independent person from reaching a similar solution; above all, knowledge sharing can generate outstanding solutions for the problems (Feledi & Fenz, 2012). Knowledge sharing may sometimes become a troublesome and challenging issue because some users refrain from sharing their knowledge with other users within the virtual community (Cabrera & Cabrera, 2005). Thus, it is very important to identify the reasons why participants share or do not share their knowledge with other subscribers of the community. If practitioners and academics could identify the basic motives and reasons for the knowledge sharing of the participants of VCs, they could obtain more accurate and insightful information about the ways they can promote knowledge sharing in information security virtual communities. Although various studies (Chan & Chan, 2011; Chu, Chan, & Tiwari, 2012; Hung & Cheng, 2012; Tsai & Cheng, 2010) have attempted to examine the knowledge sharing attitudes of the participants of VCs through different approaches,

research on the perceptions of information security professionals pertaining to knowledge sharing behaviour in professional virtual communities (PVCs) is rare.

In addition, the applicability of knowledge sharing in improving performance (Huang, 2009) and enhancing online learning (Ma & Yuen, 2011; Chan & Chan, 2011) are examined. However, there is little empirical research to determine the relationship between knowledge sharing and information security risk reduction. This is because the nature of shared knowledge in information security is different from other sectors. Knowledge in information security would be a programming code or a hyperlink, and receivers of knowledge may have to run a programming code on their computer or click on the hyperlink for knowledge. If the shared code or the hyperlink were malicious, the receivers of the knowledge would become victims of the knowledge sharing process. Feledi, Fenz and Lechner (2013), and Tamjidyamcholo et al. (2012, 2013) maintained that knowledge sharing in information security could reduce risk without doing empirical research. However, Kagal, Finin and Joshi (2003), and Furnell, Bryant and Phippen (2007) mentioned that information security knowledge sharing in virtual communities might create risk for the participants of such a community. Therefore, such contradictory notions gave us the motivation to seek a relationship between knowledge sharing and security risk reduction.

1.3 Research Objectives

The main goal of this study is to gain insights on the determinants that directly influence on information security professionals' decision to share his or her knowledge in professional virtual communities. In addition, it is to find relationship between knowledge sharing behaviour and information security risk. A set of objectives is defined to achieve the above goal. These objectives are as follows:

- To model determinants of information security professionals knowledge sharing behaviour in professional virtual communities.
- To hypothesize and test the determinants of the model integrating the direct or indirect effects of these determinants on information security professionals' willingness to share their knowledge.
- To identify and measure the dimensions of trust in information security professional virtual communities.
- To determine and measure the perceived expectation of the information security professionals in the professional virtual communities.
- To investigate the quantitative relationship between knowledge sharing behavior and information security risk reduction.

1.4 Research Questions

The following research questions guide this study:

- What determinants influence information security professional virtual communities' members to participate in knowledge sharing process?
- How do different determinants combine to influence knowledge sharing behaviour of information security professional virtual communities' members?
- How can we measure trust in information security professional virtual communities?
- How can we measure perceived expectation of participant in information security professional virtual communities?
- Is there a positive correlation between knowledge sharing behaviour and information security risk reduction?

1.5 Research Methodology

The study process model used within this research project is shown in Figure 1.1, sets out the different research activities, processes, and phases, and expected deliverables.

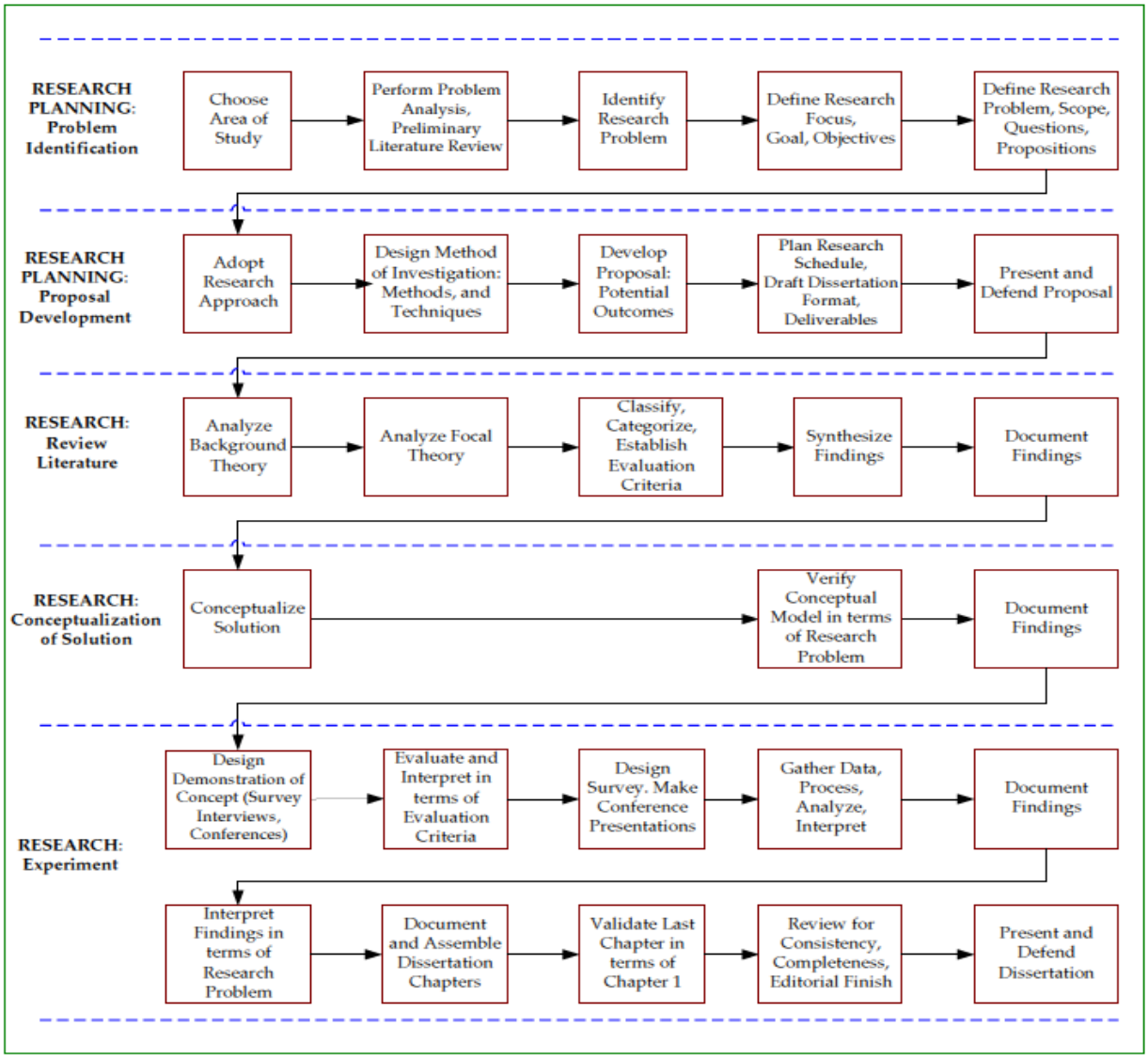

Figure 1.1 Research Process Model (Adapted from Steenkamp & McCord, 2006)

This research proposes two models to understand and evaluate the determinants of knowledge sharing behavior in information security professional virtual communities. First model explains the relationship between self-efficacy, trust, norm of reciprocity and shared language with knowledge sharing attitude. It shows that these determinants

will, directly or indirectly, develop knowledge sharing attitude and influence the intentions of participants to engage in knowledge sharing activities. With regard to this model, nine hypotheses have been examined.

Second model includes six variables: information security knowledge sharing behavior, perceived consequences, affect, social factor, facilitating condition, and risk reduction. It explains the relationship between perceived consequences, affect, social factor, and facilitating conditions with knowledge sharing behavior in information security PVCs. Furthermore, it displays the effects of knowledge sharing behavior on information security risk reduction. With regard to this model, five hypotheses have been examined.

The population of the present study consists of information security engineers and technicians in PVCs. This population included the Information Security Professional Association (ISPA), Information Systems Security Association (ISSA), Society of Information Risk Analysts (SIRA), and LinkedIn security groups. The selected PVCs provides educational forums, continuous learning framework, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Google Form technology is used to create online survey form. The link of the online questionnaires was emailed to members of PVCs. A pre-test and a pilot-test were conducted prior to performing the final and formal survey in order to validate the research instrument. Finally, two statistical tools, SPSS 19.0 and partial least squares (smart PLS 2.0), were used to test 14 hypotheses in the research models.

1.6 Research Scope

Yang & Maxwell (2011) identified different determinants influencing knowledge sharing from three perspectives: interpersonal, intra-organizational, and inter-organizational. Knowledge sharing in virtual space is mostly related to the interpersonal perspective. End users coming from all walks of life join virtual communities so as to share their knowledge relevant to common interests as well as topics. In fact, cyberspace communities work as a warehouse of knowledge that provides people with an opportunity to receive or share information.

A virtual community is a technology-oriented cyberspace, which is based upon the connections and communications of its members, and is able to create a relationship (Lee, Vogel & Limayem, 2002). Professional or technical communities are different from general virtual communities in several aspects. Bressler and Grantham (2000) asserted that a professional virtual community attracts individuals with similar and common interests who cooperate with each other in order to accomplish common goals. The evaluation of the PVCs in information security has shown that the most important challenge for knowledge sharing is motivating users to participate in knowledge sharing (Feledi, Fenz & Lechner, 2013; Fenz, Parkin & van Moorsel, 2011). This research investigates PVCs in information security. Therefore, the scope of this dissertation is limited to the knowledge sharing in information security professional virtual community.

1.7 Research Significance

Information security virtual communities are a channel that learners, technicians, and professionals through participating can advance their knowledge, solve problems, and share findings. The findings of this study are expected to benefit both researchers and

practitioners. From a theoretical point of view, first this study provides an initial step towards understanding the effect of key determinants of knowledge sharing behaviour in information security professional virtual communities. Second, this research investigates dimensions of trust and perceived consequences in information security professional virtual communities. Third, we analytically examine the effect of knowledge sharing behavior on information security risk reduction. In terms of practical significance of the study, providers and community managers of information security professional virtual communities can apply findings of this research to foster and promote the participation of members in the activities of the communities.

1.8 Dissertation Outline

This dissertation is organized into six chapters. This chapter (Chapter 1) provides an overview of the study. It outlines the background of the research, statement of research problem, research questions, research objectives, brief description of the methodological approach to the study, scope of the study, and summaries the importance of this study to both research and practice.

To clarify the relevant concepts and demarcate the topic and perspective of this study, Chapter 2 presents a literature review on information security, information security management, and information security risk management. Prior studies on knowledge sharing, information security knowledge sharing, virtual communities and professional virtual communities are also reviewed.

Chapter 3 provides the theoretical foundation for the hypotheses of the study and identifies the determinants that affect knowledge sharing in information security professional virtual communities. In addition, based on the theoretical foundation, two evaluation models proposed in chapter three.

Chapter 4 presents the research methodology used in this study. This includes the research design, determinants measures, instruments development, data collection and data analysis. Chapter 5 describes the results of the study from the statistical analyses.

Finally, Chapter 6 summarizes and concludes this dissertation. First, it provides a discussion on the studies' findings in relation to the two research models. Next, theoretical and practical contributions are outlined. Then, the conclusion remarks are explained. Lastly, the limitations and future research opportunities of this work are described.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Nowadays, the Internet allows the exchange of information through different ways, such as online group meetings, which did not exist before. Furthermore, the Internet has created virtual communities (VCs) in which users are able to share knowledge without actually seeing each other. The number of users of VCs has grown considerably, and they take part in these communities to look for necessary information to solve their problems.

In addition, many institutions and companies have turned their attention to VCs and regard them as a valuable framework that plays a major part in knowledge management (KM). They have begun to pay special attention to the advancement and progress of VCs to achieve their business goals (Chen & Chen, 2012). The usage of VCs is expanding day-by-day, and encompass various sectors, such as marketing and economics, as well as the education and social sectors (Lin, Lin, & Huang, 2008; Ma & Yuen, 2011; Teo, Chan, Wei, & Zhang, 2003). For example, in March 2000, Taiwan established a professional virtual community for teachers (SCTNet). On the SCTNet, teachers can share their professional works in terms of research results, lesson plans, and teaching resources with other community members, and receive comments and suggestions (Lin et al., 2008). As the Internet has grown and developed, VCs have come to be known as a kind of online framework. Virtual communities can be described as a social community that originated through the Internet. These communities take shape when the number of people who want to participate in public discussions increase and reach an acceptable number and when participants possess strong and sufficient emotion to build networks of personal relationship through the Internet (Vijayasarathy,

2004). These communities are built upon the inter-connections and relationships of participants.

They can generate particular scopes of information in which participants are able to perform ordinary tasks, and learn from each other and make a contribution to community knowledge, and, ultimately, they can extend the knowledge collectively (Lee, Vogel, & Limayem, 2003).Therefore, the participants of these communities can access a knowledge sharing framework and interact and communicate with each other even though they may be far away from each other geographically.

The presence of virtual communities in information security field broadens and clusters individual online activities. The fundamental step of creating a virtual community is the provision of knowledge, which can be achieved through increasing participants' willingness to share knowledge and information with other users.

2.2 Information Security

Over the years, the focus of information security has evolved from the physical security of computer centers to securing information technology systems and networks, to securing business information systems

2.2.1 Importance of Information Security

Modern society has grown to be significantly dependent on Information Systems (IS) as well as their particular associated information assets. Critical infrastructure, including power production and distribution, telecommunications, gas and oil distribution, and water distribution and purification has been powered by IS. Moreover, the driver of the global economy such as financial institutions, the governments, supply chains, and businesses reliant greatly on the IS for their very success (Jansen, 2010; McDonagh & Harbison, 2000). The importance of the information assets on their own need to be considered, even though the IS assets can be very important. Analysis indicates that the

highest damage introduced by means of an IS security breach can be losing of the strategic advantages of information and their resources (Earl, 2012; Gupta, Walp & Sharman, 2012). Despite the presence of growing attention paid for the IS and their information assets, security breaches of IS do happen, along with potentially substantial losses; both monetary, as well as compromises to information assets. While it can be difficult to determine the full extent of losses suffered through IS security exploits (Cavusoglu, Mishra & Raghunathan, 2004), threats certainly have been realized at the corporate, state, and federal levels. In 2009, the Homeland Security Information Network (HSIN) breached through compromised credentials with masses of sensitive state and federal data accessed for an unknown outcome (CSIS, 2009).

U.S. Air Force (Nakashima, 2009) released that a number of military drones operating in Iraq being compromised through the use of simple unencrypted transport mechanisms in conjunction with off-the-shelf tools (Nakashima, 2009). Moreover, In January 2010, Google disclosed that intruders had stolen information from their computers (official Google blog, 2010).

More precisely, in December 2009, the intruders sent instant messages through Microsoft Messenger Program to an employee of Google in China. The employee clicked on a link that was included in the messages and inadvertently allowed the intruders to access his/her own computer. The objective was to access Gaia, which is the famous Google software that enables users to access a range of services with one unique password. The intruders successfully retrieved passwords to access email accounts of two human rights activists in China. Later, Google discovered that dozens of Gmail accounts of other advocates of human rights in China were routinely accessed, through phishing scams or malware placed on the users' computers. This event had broad repercussions: Google decided to shut down Google China. This story

emphasizes two aspects of cyber security: malicious attackers steal information on purpose, and a user fell for social engineering.

In these examples and many others, the level of security provided to IS and its information assets can truly mean the difference between life and death. Threats to IS and information assets take many shapes and forms, and cannot always be attributed to shady hackers in dark rooms. These examples are just a few of many, all with varying threat vectors and vulnerabilities exploited. However, the scenarios fundamentally underline the problems that face corporate entities and nation-states as their infrastructures become increasingly technological and enemies become increasingly sophisticated in their attack techniques. To combat these threats, a number of prescriptive IS security programs with varying content have been developed .These programs all differ in breadth and scope, but they have one common aim: securing IS and information assets.

2.2.2 Evolution of Information Security

Most organizations mainly emphasized on physical protection of their assets prior to development of computer security in to their numerous dimensions of these days. In the early years of computing, protecting and securing data coming from natural disasters or perhaps malicious activities was consideration of organizations with computers. Security objectives ultimately changed to computer security by arriving of personal computers. The strategies of computer security evolution are shown in Figure 2.1.

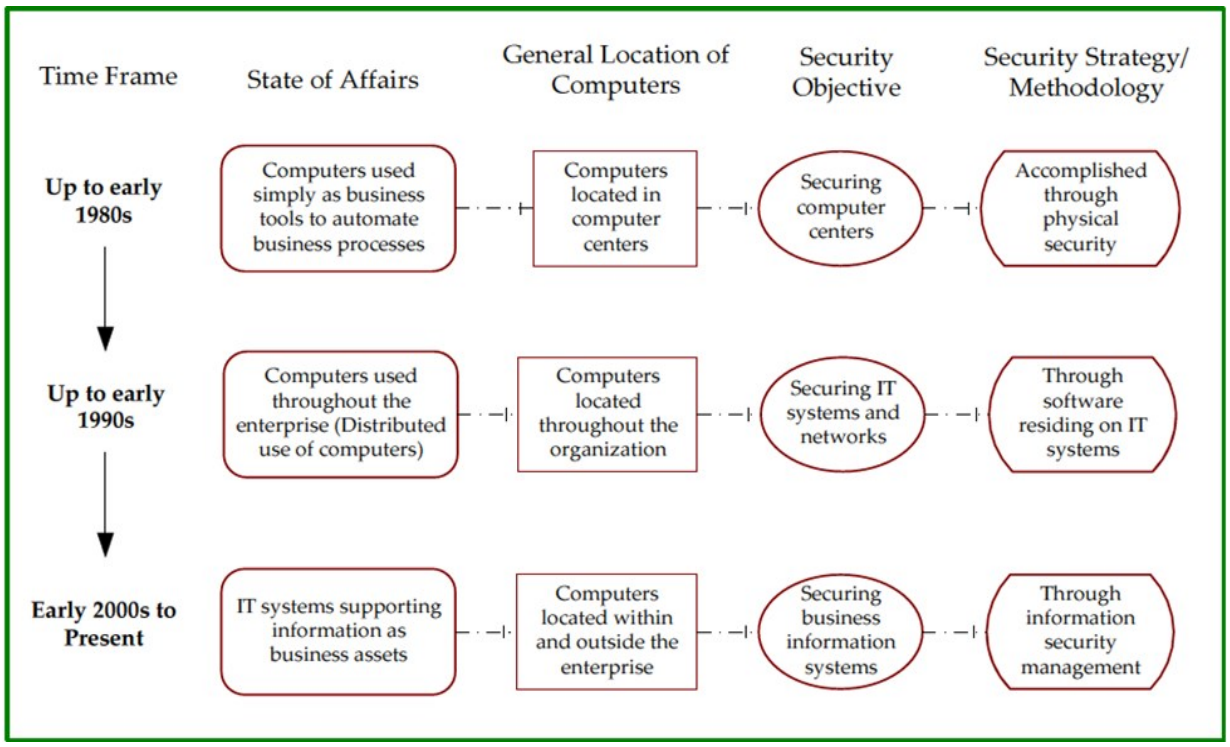

Figure 2.1 Evolution of Computer Security Strategies (Developed from Vermeulen and Solms, 2002)

In recent times, the information security focus has evolved from the physical security of computer centers to securing networks and information technology systems, in order to securing information systems of business. Due to the fact that computer centers have evolved into data centers, they house a number of databases and servers. These types of databases consist of information and data which is certainly essential to the profitability and economical success of the enterprises. After a while, computer architecture developed from stand-alone environments to networked computer systems. The actual advancement of networked systems signalled in a completely new era within computer communications. The advent of the Wold wide web and this expansion of computer networks added an additional aspect to the information security. Using the Internet, computer systems can easily connect and share information along with other computers beyond an organization's networks and outside their computer center.

According to Eloff and Solms (2000) information security has developed by means of three waves. The initial wave named the “technical wave” which is shown with a technical approach to information security. The next trend called the “management wave” which features an increasing interest and engagement from management to safeguard information. The third trend named the “institutional wave” which adopted the codes of conduct and best practices. Management is concentrated upon indicating the information security power of the organization through applying information security in to the organizational culture, certification, and continuous measurement and monitoring. Solms (2006) named fourth wave the “Information Security Governance”. Information Security Governance is actually greater than simply information security management. Security Governance obviously signifies the considerable function associate with Boards of Directors and top management in the manner information security is dealt with inside an organization. Information Security Governance is actually a fundamental element of Corporate Governance. Security Governance includes: the Board and Top management commitment towards good information security; the correct organizational structures with regard to enforcing very good information security; complete individual awareness as well as dedication in direction of proper information security; and the required policies, processes, technologies, procedures along with compliance enforcement mechanisms; almost all operating collectively to make sure that the availability, integrity and confidentiality of the company’s digital assets are continually managed and maintained. Therefore, Information Security Governance entails everybody inside a company – from the Chairman of the Board through to the data entry clerk on the shop floor and the driver of the vehicle delivering the products to the customers. Information Security Governance is seen as the general manner in which information security as being a discipline can be handled to minimize IT risks.

2.2.3 What Is Information Security?

The term ‘information security’ is often used interchangeably with ‘computer security’. Baskerville (1988) defines ‘computer security’ as purely the protection of electronic computer and communication systems, i.e. a concern with the security of technology. He defines ‘information security’ as a wider range of concerns, comprising computer system security, systems design and analysis methods, manual information systems, managerial information security concerns (for instance policies of security) and ethical and societal issues.

In this research, we particularly concentrated on information security (InfoSec) and following section will explain different view of information security. Anderson (2003) “defined information security as a well-informed sense of assurance that information risks and controls are in balance.” Peltier (2005), an additional well-known writer and instructor in InfoSec, declares that, “InfoSec encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets.” In 2010, ISACA defined information security as something that: ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability).

Whilst a number of definition of the term information security has been proposed, this particular research uses the definition of Whitman and Mattord (2011) which is based on Committee on National Security Systems(CNSS), formerly known as the National Security Telecommunications and Information System Security Committee (NSTISSC): “InfoSec is the protection of information and its critical elements, including the systems

and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology.

2.2.4 Threats to Information Security

Those accountable for the information in organization need to start with an understanding from the threats dealing with the information so as to reinforce the degree of protection of information in the organization. They have to take a look at the vulnerabilities built in the systems which transfer, process, and store the information probably afflicted to those threats. The detection of the prominent threats dealing with organizational information security is the very first part of this plan, and accordingly the ranking of those threats so as to enable organizations to direct priorities. Whitman and Mattord (2010) conducted a survey and classified the threats into 14 categories and ranked them in order of severity:

1. Unauthorized data collection and/or access (Deliberate Acts of Trespass or Espionage)

2. Viruses, Trojan horses, worms, Tap Door or Back Door, macros, Polymorphism (Deliberate Software Attacks)

3. Employee mistakes or accidents (Act of Human Failure or Error)

4. Incomplete, Inadequate or Missing Organizational Planning or Policy

5 Incomplete, Inadequate or Missing Controls

6. Illegal confiscation of information or equipment (Deliberate Acts of Theft)

7. Copyright, piracy infringement (Compromises to Intellectual Property)

8. Destruction of information or systems (Deliberate Acts of Vandalism or Sabotage)

9. Unknown loopholes, code problems, bugs (Technical Software Errors or Failures)

10. Equipment failure (Technical Hardware Errors or Failures)

11. Earthquake, Landslide or mudslide, fire, flood, Hurricane or typhoon, lightning, Tornado or severe windstorm, Electrostatic discharge (ESD), Tsunami, Dust Contamination (Forces of Nature)

12. Communication and other Service Provide Issues, Internet Service Issues, Power irregularities (Deviation in Quality of Service)

13. Outdated or antiquated technologies (Technological Obsolescence)

14. Blackmail of information disclosure (Deliberate Acts of Information Extortion)

On behalf of (ISC)2, Ayoub (2011) carried out a survey which showed, since 2008, numerous technology trends have moved into the mainstream. Capturing the trends that have a great impact on information technology is important to measure the effect on the information security profession. The three primary new technology trends studied in detail in 2010 were mobile devices and mobility, cloud computing, and social media. These new technology areas also represent the greatest risks to organizations. Figure 2.2 shows the top security threats to organizations in order of severity. Ayoub (2011C) believes this illustrates the ubiquity of modern threats.

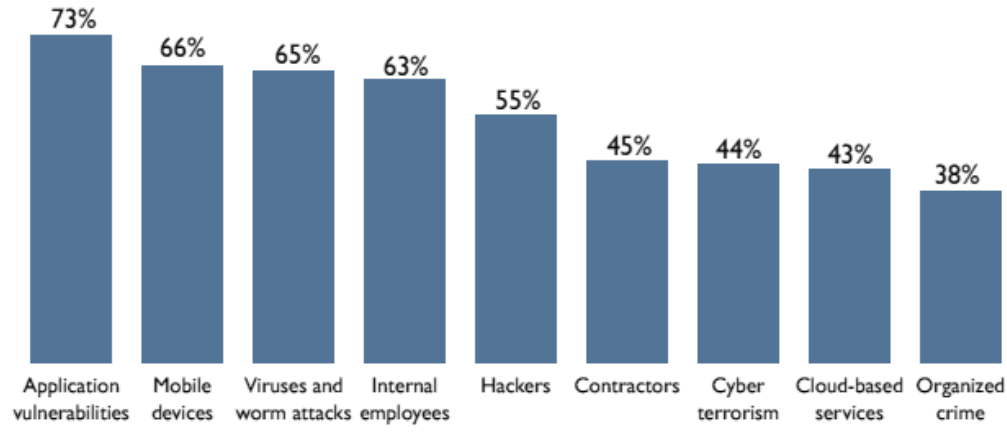

Figure 2.2 Top Security Threat Concerns

2.2.5 Security Technologies

Information security is a discipline in which combination of policy, procedures, education, training, awareness, technology, and the efforts of people exist to improve the availability, integrity, and confidentiality of an organization's information assets. Technical controls alone cannot secure an IT environment, but they are usually an essential part of information security programs (Whitman & Mattord, 2011). The sections that follow will give the information security technologies available based on Venter and Eloff (2003) categorization, after which each technology is briefly explained.

- Cryptography: Basically, cryptography is 'hidden writing'. It is scientific disciple to protect confidentiality and integrity of data (Scambray et al, 2001). Encryption is the procedure of scrambling or transforming a cleartext message in order that it becomes a ciphertext message. Synonyms used for encryption are usually encipher and encode. Decryption is the reverse process of encryption. Decryption is the process of rearranging the ciphertext so that a ciphertext message is transformed into a cleartext message. Synonyms used for decryption are usually decipher and decode.
- Digital signatures: A digital signature can be thought of as the equivalent of a handwritten signature with the same goal: associating a mark that is unique to an individual with a body of text (Pegrum, Jamieson& Yuen, 2003). In the same way as a handwritten signature, a digital signature must not be forgeable, in other words only the legitimate sender of a message should be able to create the digital signature (King, Dalton, & Osmanoglu, 2001). Digital signatures are created using cryptographic algorithms.
- Digital certificates**:** The challenge associated with trust on the Internet attempt to be resolved with Digital certificates. Trusted third parties are issuing Digital

certificates, and also it is referred as CAs (Certificate Authorities) (Tiwana, 1999). CAs is actually business oriented corporations that attest to the particular identities of individuals as well as corporations on the Internet. Thus, a new network of trust is actually founded amidst Internet users.

- Virtual private networks: Virtual private network (VPN) is closely associated with cryptography .VPN is kind of technology to encrypts network traffic. The VPN makes it possible for a corporation with several websites to have connection between these kinds of websites on the public network, for example the Internet. The advantage of VPN is that the all data packets traveling among the websites are secured and encrypted (Venkateswaran, 2001). Furthermore, the VPN technology can be used to restrict the packets travelling between the organization's websites. However, there is a difference between function of normal encryption and VPNs. In the encryption, the data is usually encrypted simply when it is transported on the public network, but in the VPN, the data which moves between the originating host and the VPN host is not encrypted. Moreover, if data comes from an authenticated host, it will simply be encrypted through the VPN.
- Vulnerability scanners: Signatures has been used for identifying vulnerabilities in Vulnerability Scanners (VSs). Hence, a vulnerability scanner is a new sort of information security technology that is of a specific scenario of intrusion detection (Horng, et al., 2011). Due to fact that hosts over a network are usually scanned in particular times and rather than constantly, Vulnerability scanning is generally known as interval-based scanning. It is called a snapshot when VS has finished a scan and sampled the data in to a report.
- Anti-virus scanners: Serious damages have been triggered by computer viruses on the net during the past decade. A piece of malicious software program that

has the capacity to recreate itself throughout the Internet, once activated, is computer virus (Endler & Collier, 2007). For that reason, anti-virus scanners have been created in order to deal with computer viruses. Viruses and functions have been scanned by anti-virus scanners prior to they might trigger havoc. The operation of anti-virus is significantly in the same manner as VSs in that they additionally 'know' what a particular signature of virus looks like.

- Security protocols: Internet Protocol Security (IPSec) and Kerberos are examples of security protocols. There are different protocols which they can be categorized as information security technologies. These kinds of protocols are technologies that make use of a standard procedure for controlling data transmitting among applications or computer systems to guard hypersensitive information prior to such information could be intercepted by means of intruders.
- Security hardware: Hardware routers or hardware encryption modules are examples of security hardware. Physical hardware devices which have been used to perform security tasks are called security hardware. Security hardware has been implemented to prevent an intruder from changing or modifying the hardware devices.
- Security SDKs: Microsoft .NET SDKs and Java security manager are examples of Security software development kits (SDKs). The SDKs are programming tools that can be used to create security programs. The SDKs are forms of computer software which can be used to construct security applications for example Web-based authentication programs.
- Firewalls: Firewalls are viewed as the initial line of protection in an attempt to keep out intruders (Pabrai & Gurbani, 1996). The World Wide Web firewall is a software program which sets up on especially configured computer system in

which acts like a filter, blockade, or bottleneck among an organization's internal or trustworthy network and the untrusted network or the net (Mayer, Wool & Ziskind, 2000). Preventing unauthorized communications inside or outside of the organization's host or internal network is the main objective associated with firewall. A new type of firewalls in the security arena is personal firewalls. Personal firewalls, in contrast to traditional firewalls, are installed over a typical workstation and make an effort to simply safeguard that certain workstation from all of those other hosts on the Internet or the network.

- Access control: The purpose of access control is actually to make sure that a subject possesses adequate rights to accomplish a number of activities over a system (Sandhu & Samarati, 1994). A service, an application, user, or a group of users, can be potentially a subject. In a system subjects can have various levels of access to specific objects. A printer, a file, a process, or a directory might be an object.
- Passwords: A password can be used to gain admission as well as access to information for example a computer system, a file, or application. Sequence of characters, a secret word, or phrase is named as a password.
- Biometrics: Biometrics makes use of the geometry of a particular section of a human body to authenticate an individual. Different kinds of biometrics exist and they have been utilized by many organizations, for instance fingerprint, hand, voice recognition biometrics and retina.
- Intrusion detection systems: The procedure of checking the actual events which take place within network or a computer system and examining them with regard to signals of intrusions is intrusion detection. Any kind of activities that try to compromise the availability, integrity, or confidentiality of the resources is called an intrusion. An intrusion detection system (IDS) is hardware or software

technologies that automate the analysis and monitoring process (Pietro & Mancini, 2008).

- Logging: Logging makes attempts to assemble information on a number of events that occur as an information security technology. The objective of logging would be to provide audit trails which are often tracked following a security event has occurred.
- Remote accessing: Remote accessing can be kind of an information security technology that enables processes or people in order to gain access remote services. Nevertheless, access is not constantly managed to remote services due to fact that it's possible to gain access the remote service anonymously. In cases like this, being able to access remote services anonymously presents some sort of threats. For instance, when unknown internet connections shouldn't actually be permitted in accordance with an organization's security policy, a few computer systems might be mistakenly configured to permit unknown connections automatically.

15th annual Computer Crime and Security Survey (Richardson, 2011) was conducted by Computer Security Institute (CSI) showed (see Figure 2.3) what security technologies companies have deployed to protect their organizations. Invariably and not surprisingly, anti-virus systems and firewalls have topped the list.

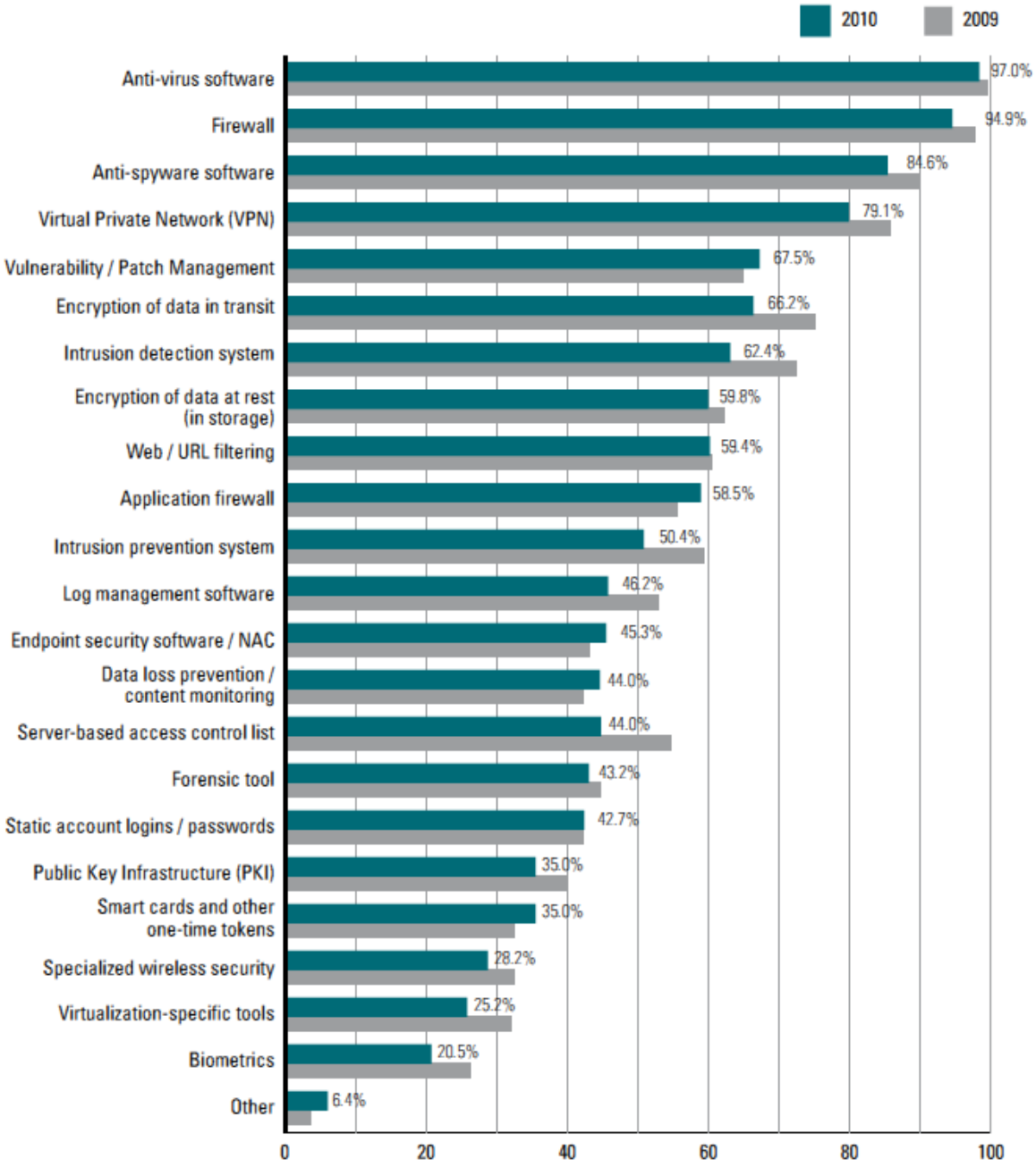

Figure 2.3 Types of Security Technology Used by Percentage (Richardson, 2011)

2.3 Information Security Management

These communities of interests which are in charge of the security of an organization's information assets need to model a functional security strategy, after which put into action a management model to implement as well as maintain that strategy (Whitman & Mattord, 2009). An information security management (ISM) model establishes and maintains a secure information environment (Dlamini, Eloff & Eloff, 2009). Vermeulen

and Solms (2002) defined ISM as the organized procedure for the execution along with administration of information security in an organization. The ISO/IEC 27001 standard defines ISM as the main part of the general management system that implements, establishes, operates, reviews, monitors, maintains, and improves information security (Humphreys, 2006).

The primary goal of an ISM is to ensure the security of information through proactive management of information security risks, threats and vulnerabilities (Kritzinger & Smith, 2008). An ISM requires that appropriate policies, procedures, standards, and guidelines are implemented to provide proper balance of security controls and business objectives, and its adoption allows organizations to demonstrate their commitment to secure business practices (Siponen & Willison, 2009; Tipton & Henry, 2006). Others described some characteristics of effective security management in the organizations, which include:

1. Preserving a safe functioning atmosphere, such as an operational infrastructure and responsive technology (ISO/IEC 17799, 2000).

2. Keeping an up-to-date security policy which has been written (ISO/IEC 17799, 2000; Solms & Solms, 2004).

3. Performing a formal and proper risk management process (ISO/IEC 17799, 2000; Saint-Germain, 2005; Peltier, 2005).

4. Providing sufficient security instruction as well as awareness to end users (ISO/IEC 17799, 2000; Solms & Solms, 2004).

5. Setting up a security governance framework that is certainly incorporated with entire organization governance framework (ISO/IEC 17799, 2000; Solms & Solms, 2004; Solms, 2006).

6. Compliance with regulatory and statutory needs, in addition to established organization security standards (ISO/IEC 17799, 2000).

Over the past several decades, numerous information security management standards and guidelines have been developed by various industry groups and standardization bodies. The most prominent of these standards and models are:

- ISO/IEC 2700x family of information security management system (ISMS) standards and guidelines (BS 7799-1 and BS 7799-2, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27008, ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27013ISO/IEC 27014, ISO/IEC 27015)
- ISO/IEC 21827:2008 Capability Maturity Model (SSE-CMM)
- Generally Accepted Information Security Principles (GAISP)
- Generally Accepted Systems Security Principles (GASSP)
- Information Security Forum (ISF) Standard of Good Practice for information security (SoGP)
- Guidelines for the Management of Information Technology Security (GMITS)
- Organization for Economic Cooperation and Development Guidelines for the Security of Information Systems and Networks
- NIST Security Model (800-12,800-14,800-18,800-26,800-30,800-53 Revision 3)
- U.S. Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
- COBIT 5.0(2012) (Control Objectives for Information and related Technology) has three main components –so called GRC-Governance, Risk management and Compliance.
- COSO (The Committee of Sponsoring Organizations of the Treadway Commission)

In all of the information security management models and standards (Nnolim, 2007) information security risk management (ISRM) plays an important and prominent role.

ISO 27005 (2008) proposed that ISRM have following purposes: promoting an ISM, preparing of an incident response program, preparing of an enterprise continuity plan, complying with legal and evidence of due diligence, and explanation of the information security prerequisites for a service, product, or a mechanism. Some researchers introduce it as a synonym for ISM, as a result in the next section ISRM to be detailed.

2.4 Information Security Risk Management

On account of the increasing breaches that impact the protection of information resources and accordingly the business activities, the significance of coping with information security risks is maintaining growth worldwide. It is clear that businesses are possibly suffering the loss of revenue due to the lack of an efficient information security risk management programs which proactively sharing to protect the enterprises' information resources. For that reason, companies are necessary to obtain and operate an efficient information security risk management program to not only attain superior safety of their information resources and subsequently slow up the monetary cutbacks, and also adhere to the particular governmental mandatory regulations and laws that has been applied within their surroundings (Fenz & Ekelhar, 2011).

Wheeler (2011) pointed out that there is no single perfect way to organize organization security program or reporting structure, but it is clear that risk management program needs to be the umbrella for all the daily security activities. To have a successful information security program, an effective risk management process should be considered as an important component (Initiative, 2011).

The process of figuring out vulnerabilities within an organization's information systems as well as taking very carefully reasoned actions in order to make sure the availability, integrity, and confidentiality of all of the elements in the organization's information system is named risk management (Whiteman & Matthord, 2011). Generally, Microsoft

(2006) defined security risk management process as the entire attempt to control risk to an appropriate and acceptable levels throughout the organization. Basically, the objective of risk management is to minimize possibility of unpredicted damaging outcomes, while maximizing the output of the business with regards to revenue, services, and products (Wheeler, 2011).

Risk management is often considered alongside governance and policies (McFadzean, Ezingeard & Birchall, 2006; Dunkerley & Adviser-Tejay, 2011). When attempting to create a balanced IS security program, research has shown that the security risks of the organization must be considered alongside the organizational strategies (Kotulic & Clark, 2004; Dunkerley & Adviser-Tejay, 2011). Risk management is a multifaceted, complex task that needs the engagement of the whole organization—from senior executives / leaders providing the top-level goals and objectives and strategic vision for the organization; to mid-level leaders managing, planning, and executing projects; to persons on the front lines performing the information systems supporting the organization's business functions / missions (Initiative, 2011).

These days, there are different types of information security risk management models including NIST 800-30 (NIST,2002), Microsoft Risk Management Approach (Microsoft, 2006), ISO/IEC 27005 (2008), OCTAVE (Alberts, Dorofee, Stevens, & Woody, 2003), and CRAMM (2001); each one of these methods include various steps and view with regard to determining, analyzing, evaluating, managing and keeping track of risks to information systems. The subsequent sections offer an overview of ISO/IEC 27005 (2008) method for information security risk management, ISO/IEC 27005 is most commonly used and well-known standard for ISRM.

2.4.1 ISO/IEC 27005

Guidelines for information security risk management within an organization have been provided by ISO/IEC 27005. In particular, ISO/IEC 27005 supports the certain requirements of an information security management system (ISO/IEC 27005, 2008). Figure 2.4 shows the summary of ISO/IEC 27005 process framework. The process of information security risk management consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review. Firstly, the framework or context is established. After that the risk assessment is carried out. If this gives adequate information to be able to efficiently figure out those things required to modify the risks to a satisfactory degree then the job is finish along with the risk treatment method employs. An additional iteration of the risk assessment with modified context will be carried out if the information is inadequate (see Figure 2.4, Risk Decision Point 1).

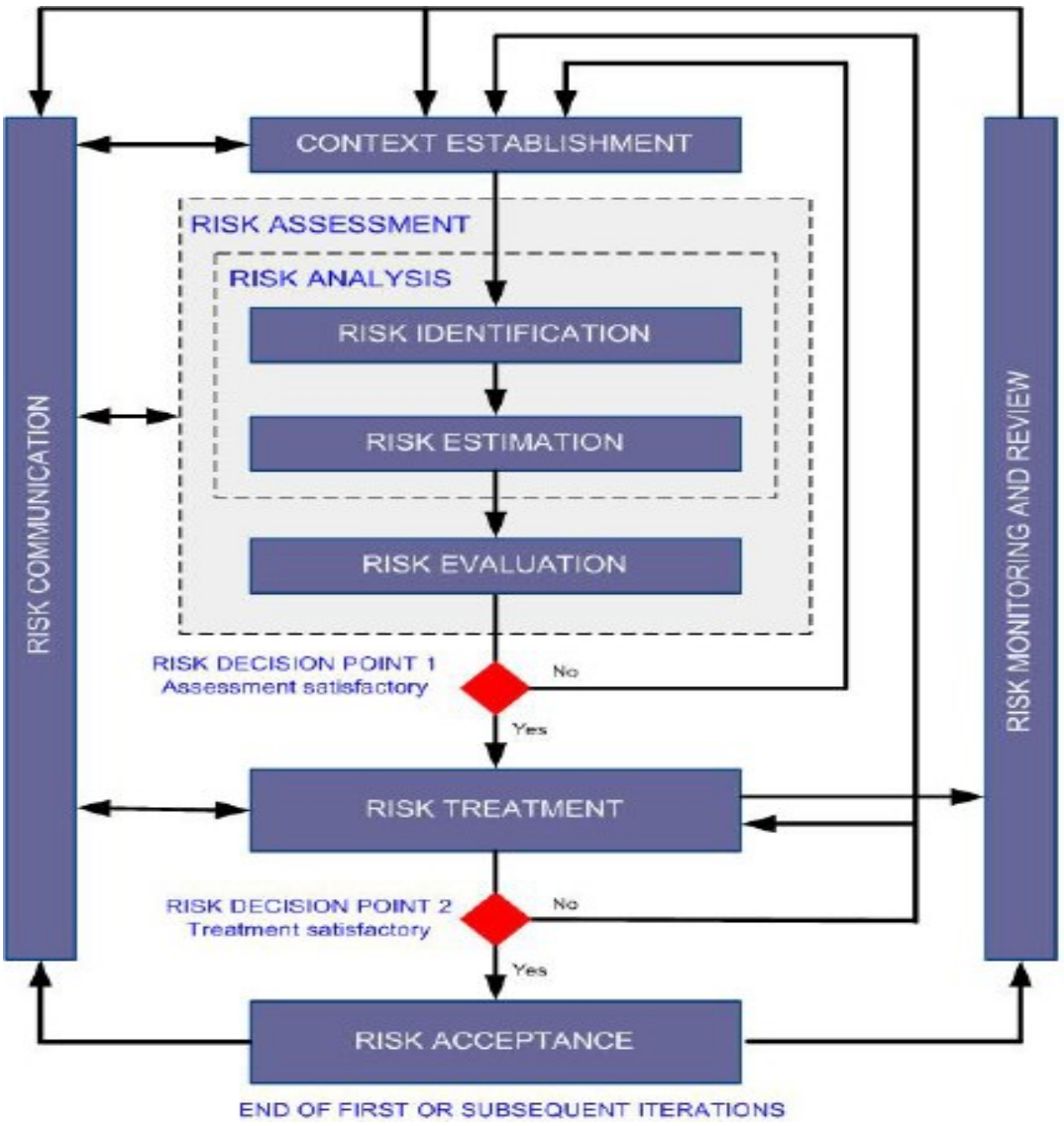

Fig. 2.4 Information Security Risk Management Process (adapted from Singh, 2009)

The purpose of this research is to investigate risk communication concept in risk management process. Risk communication is usually an activity to attain agreement about how to control and manage risks by sharing and/or exchanging information about risk between the stakeholders and other decision-makers. The information can be, but is not restricted to the nature, form, existence, severity, likelihood, acceptability, and treatment of risks. Efficient communication and connection amongst stakeholders is essential because this might have a substantial effect on decisions that needs to be made. Communication will make certain that those people accountable for applying risk

management, and also those people with a vested interest realize the foundation why specific actions are needed and on which decisions are made. Communication can be bi-directional. Perceptions associated with risk can differ because of variation in presumptions, needs, concepts, problems and concerns of stakeholders since they connect with risk or the issues under discussion. Stakeholders according to their perception of risk are more likely to make judgments on the tolerability of risk. This is particularly essential to make sure that the stakeholders' perceptions of risk, along with their perceptions associate with benefits, can be determined and recorded and the underlying reasons clearly understood and addressed. Risk communication should be carried out in order to achieve the following (ISO/IEC 27005, 2008):

- To provide guarantee with the result of the corporation's risk management
- To gather risk information
- To share the outcome of the risk assessment process and also present the treatment plan of risk
- To prevent or minimize both happening and consequence of information security breaches as a result of lacking mutual understanding between stakeholders and decision makers
- To support decision-making
- To obtain new knowledge and information related to security
- To cooperate with other parties as well as plan reactions to minimize effects of any incident
- To give a feeling of accountability regarding risks to stakeholders and decision makers
- To enhance awareness

For regular operations and also for emergency situations, organizations ought to create risk communication plans. As a result, risk communication activity need to be carried

out constantly. The coordination among stakeholders and main decision makers can be accomplished through the creation of a committee or panel in which discussion about risks, their particular prioritization and suitable treatment, and acceptance may occur.

It is necessary to interact with the appropriate communications unit or public relations inside the firm to coordinate all responsibilities associated with risk communication. This is essential and crucial in case of crisis communication actions, for instance, in reaction to specific incidents.

Risk communication is another name for knowledge sharing or information sharing. Others documents and standards such as Microsoft (2006), NIST Special Publication 800-53 Revision 3 (Ross, Katzke, Johnson, Swanson & Stoneburner, 2008), NIST Special Publication 800-137 (Dempsey, 2011) is used knowledge and information sharing as a synonym for risk communication.

2.5 Knowledge Sharing

As knowledge management (KM) is gaining more strategic significance in organizations and institutions, these organizations have turned to applying different KM initiatives. Lin, Wu and Lu (2012)) discerned a number of fundamental factors in KM activities, which include recognition, collection, selection, organization, implementation, sharing, and construction of knowledge. Knowledge sharing is considered as a critical step for successful knowledge management

2.5.1 Definition of Knowledge

Historically, from a philosophical perspective, knowledge is defined as "justified true belief (Huber, 1991; Nonaka, 1994) that enhances an entity's capacity for effective action (Alavi & Leidner, 2001). Drawing upon the work of Polanyi (1962), Nonaka (1994) explicates two dimensions of knowledge: tacit and explicit. Tacit knowledge is rooted in action, experience, and involvement in a specific context, while explicit

knowledge can be articulated, codified, and communicated in symbolic form or natural language (Alavi & Leidner, 2001). These two dimensions of knowledge are not dichotomous states of knowledge, but rather are mutually dependent and reinforcing qualities of knowledge. Another question that arises is, what is the difference between knowledge and information? The assumption may be that if knowledge is not something different from information, then there is nothing new or interesting about knowledge management (Fahey & Prusak ,1998).

2.5.2 Data, Information and Knowledge

Some authors address the question of distinguishing among knowledge, information and data. A commonly held view is that data is raw numbers and facts, information is processed/interpreted data, and knowledge is authenticated/justified information (Machlup, 1980). Knowledge derives from information as information derives from data (Davenport & Prusak, 2000). But this hierarchy from data to knowledge is also argued to be inversed. For example, Tuomi (1999) argues that knowledge must exist before information can be formulated and before data can be measured to form information. Furthermore, some scholars posit that information is converted to knowledge once it is processed in the mind of individuals and knowledge becomes information once it is articulated and presented in the form of text, graphics, words, or other symbolic forms (Alavi & Leidner, 2001). However, from these views, the key to effectively distinguishing between information and knowledge is still not clear (Alavi & Leidner, 2001).

By contrast, some scholars emphasize the strong association between information and knowledge (Detlor, 2002). For example, Schultze (2000) describes the close relationship between information and knowledge as a "dialectic, mutually constitutive relationship." Especially in practice, it is quite difficult to separate them unambiguously

(Tuomi, 1999). Similarly, Kogut and Zander (1992) include both tacit "know-how" and information "know-what" in their definition of knowledge.

How knowledge is transmitted between knowledge providers and receivers sheds light upon the tight association between information and knowledge. As such, the next subsection of this thesis discusses the process by which knowledge is exchanged between individuals over communication channels. Specifically, the goal is to describe how knowledge is shared over electronic communication mediums - the channel found and utilized by knowledge sharers in online communities.

2.5.3 Knowledge Providers, Receivers and Communication Mediums

Regarding to knowledge sharing, two actors (entities) are involved: a knowledge provider and a knowledge receiver. A knowledge provider refers to an individual who provides or shares his or her knowledge with others, while a knowledge receiver refers to the one who receives or acquires the knowledge from the other person. Other scholars use similar terms to describe these two concepts. For examples, Wasko and Faraj (2005) use the terms knowledge contributor and knowledge seeker, Chiu, Hsu, and Wang (2006) utilize the terms knowledge contributor and knowledge receiver, Hew and Hara (2007) use the terms knowledge provider (sharer) and knowledge seeker, and Peddibhotla and Subramani (2007) utilize the terms knowledge contributor and knowledge user.

In addition to the knowledge provider and receiver, there is a communication medium through which knowledge is transferred from the provider to the receiver. Other scholars refer to this concept as a transmission channel (Gupta & Govindarajan, 2000) or as a transfer mechanism (Alavi & Leidner, 2001). In online communities, the communication medium can be a bulletin board system or a chat room.

Conceptualized based on prior work (Alavi & Leidner, 2001; Gupta & Govindarajan,

2000) and adapted to the online community context, Figure 2.5 illustrates the knowledge sharing process in which a knowledge provider, recipient and communication medium are involved. The process of knowledge sharing in virtual communities consists of two stages.

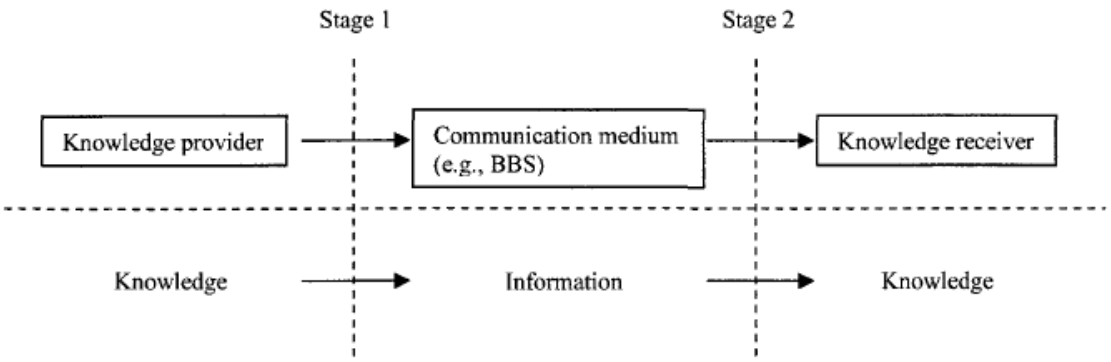

Figure 2.5 Process of Knowledge Sharing in Online Communities (Conceptualized based on Alavi & Leidner, 2001)

In the first stage, the knowledge provider shares his or her knowledge by posting information on a communication medium (CM). In this stage, the knowledge embedded in the head of the individual is converted to information (e.g., text posted on the communication medium). What is posted on the CM is information. And what is provided by the knowledge provider is knowledge. It is something embedded in the mind of the individual before it is converted to information, and also because it is a "justified belief (Huber, 1991; Nonaka, 1994). When an individual answers another person's question based on his or her own experience and accumulated knowledge, this answer is a justified belief; that is, this individual provides an answer that he or she believes to be correct. Thus, what is shared by the individual is knowledge, although what is posted on the CM is information. In the second stage, the knowledge receiver reads the information posted on the CM, and then creates his or her own knowledge. In

this stage, information is converted to knowledge that resides within the mind of the individual.

2.5.4 Knowledge Sharing or Information Sharing

As illustrated in Figure 2.5, what is possessed in the mind of a knowledge provider and receiver is knowledge, while what is posted on a CM is information. This raises the question: should this process be called knowledge sharing or information sharing in online communities? As mentioned above, three entities (i.e., the knowledge provider, the communication medium, and the knowledge receiver), are involved in this process. From the communication medium's perspective, this process can be called information sharing since what is posted and stored in the CM is information.

But from the knowledge provider's perspective, as mentioned above, what the individual provides is knowledge since it is something embedded in the head of this individual and is justified by the individual to be correct (at least the individual believes it to be so).

Thus, from the knowledge provider's perspective, this process is known as knowledge sharing. As mentioned earlier, this thesis is mainly concerned with the willingness of individuals to share with others the knowledge they have acquired or created. Therefore, this study is from a knowledge provider's perspective. Thus, it is more appropriate to call this process knowledge sharing rather than information sharing. In addition, previous studies in online communities, especially the recent ones, use the phrase "knowledge sharing" (for example, Wasko and Faraj (2005), Chiu et al. (2006), Ma and Agarwal (2007), and Hew and Hara (2007)).

Additionally, what is posted on a CM is also regarded as explicit knowledge of the virtual communities (Bieber et al., 2002). This point is consistent with the view of knowledge embedded in physical systems, such as databases (Holsapple & Joshi, 2004).

For example, Kankanhalli, Tan and Wei (2005) regard the information input and stored in electronic knowledge repositories as knowledge. Based on this view, even from the communication medium's perspective, the sharing process mentioned above can also be called knowledge sharing.

2.5.5 Empirical Research on Knowledge Sharing

In recent years, a number of studies have focused on knowledge sharing, mostly in organizational research and typically using different theories. Some of these studies are highlighted here. Several studies (Tamjidyamcholo, Bin Baba, Tamjid & Gholipour, 2013;Casimir, Ng, & Cheng, 2012; Ford, 2005) used the theory of reasoned action and/or its extension, the theory of planned behavior, to explore knowledge sharing.

Jeon, Kim, and Koh (2011) used the theory of planned behavior in combination with the theory of motivation (intrinsic and extrinsic motivation) and the Triandis model (an extension of the theory of reasoned action) (Triandis, 1980). The theory of reasoned action maintains that human behavior is impacted by attitudes, subjective norms, and intentions. The motivation theory differentiates between intrinsic and extrinsic motivations, and the Triandis model argues that human behavior is determined by the individual's intentions, which, in turn, are influenced by social factors, affect, and perceived consequences. Additionally, behavior is determined by the presence or absence of facilitating (or debilitating) conditions.

Ford (2005) conducted a study with 46 participants using mixed methods to identify the relationships between attitudes, subjective norms, intention to share, and actual knowledge sharing. The results of the study suggest that the theory of reasoned action does help to explain the actual knowledge sharing behavior, although approximately 86 to 87% of variance in actual knowledge sharing behavior did not seem to be predicted

by intentions. Additionally, the results suggest that perceived behavioral control is not a significant predictor of intentions or of actual knowledge sharing.

Chen and Chen (2009) studied the relationships between social network times, learners' attitudes towards knowledge sharing, their web-specific self-efficacy (beliefs in their capabilities of performing online knowledge sharing), their subjective norms, and their actual knowledge sharing behavior, as well as whether the knowledge sharing behavior mediated these relationships. The participants in the study were 369 full-time senior college students and MBA students. The results of the study suggest that attitude, subjective norms, web-specific selfefficacy, and social network times are good predictors of knowledge sharing intention. Knowledge sharing intention is significantly associated with knowledge sharing behavior, whereas knowledge creation self-efficacy has not been found to significantly impact knowledge sharing intention.

Wu and Wei (2010) studied the relationships between subjective norms, expected contributions, expected loss, distinctiveness, altruism, positive reinforcement, expected relationships, sharing interference, and knowledge sharing attitudes of 250 participants from four universities in Taiwan. The results of the study suggest that subjective norms, expected contributions, expected loss, distinctiveness, and altruism influence knowledge sharing attitudes; whereas positive reinforcement, expected relationships, and sharing interference have no significant influence.

Casimir et al. (2012) studied the relationship between intention to share and knowledge sharing using, information technology usage as a mediator/moderator variable. The participants in the study were 483 full-time employees from 23 organizations. The results of the study suggest that information technology usage mediates the relationship between intention to share and knowledge sharing behavior.

Majchrzak, Rice, Malhorta, King, and Ba (2000) conducted a case study using adaptive structuration theory (DeSanctis & Poole, 1994) to investigate technology adaptation in

interorganizational virtual teams whose task was to create a highly innovative product over a ten month period. The theory examines the change process from two vantage points: (a) the type of structures that are provided by advanced technologies, and (b) the structures that actually emerge as people interact with these technologies. A central aspect of the study was the question, what helps knowledge sharing (what is shared and what furthers sharing)? The results of the study suggest that, in situations when the virtual teams face discrepant events, they adaptively use technology for effective collaboration.

Sole and Edmondson (2002) used the situated knowledge perspective in a longitudinal qualitative study to explore processes of acquiring, sharing, and applying knowledge in teams with members from different locations and occupations—especially how virtual teams might overcome challenges created by functional boundaries and geographic dispersion in order to accomplish ambitious project goals. According to this perspective, knowledge is dispersed among team members, and teams benefit from the fact that dispersed teams can leverage local skills and resources. The findings of the research suggest that dispersed teams highly valued learning, but the ease of learning depended on differences in team members' awareness of relevant situated knowledge and how readily that knowledge could be appropriated.

Lichtenstein and Hunter (2004) conducted two exploratory case studies of knowledge sharing using receiver theory. This theory argues that it is the receiver's needs and behavior rather than the sharer's needs that drive the knowledge sharing process. The results of the study suggest that sharers tend to share knowledge when they believe that the receiver is ready.

Ardichvili et al.(2006) conducted a qualitative study with 36 managers and employees in three countries—Brazil, China, and Russia—to explore the impact of cultural factors (degree of collectivism, competitiveness, importance of saving face, in group

orientation, attention paid to power and hierarchy, and culture-specific preferences for communication modes) on knowledge sharing in virtual communities of practice. The results of the study suggest that the above-listed factors have different levels of importance for knowledge sharing in different countries. For instance, saving face was found to be less important in China than expected, whereas modesty and competitiveness were found to be serious barriers to information sharing in China, but not in Russia and Brazil. Perceived differences in power and hierarchy were found to be less critical in all three countries than initially assumed.

Liao (2006) used the social power framework (French & Raven, 1959) to study the relationships between the power of teachers (e.g., reward, punishment, and legitimacy), interaction (learners' perceived degree of interaction with other learners), knowledge sharing, and learning satisfaction for 103 undergraduate students enrolled and studying in a distance learning course. The results of the study suggest that learning satisfaction has a direct relationship with knowledge sharing, whereas interactions do not have a significant relationship with learning satisfaction; and the teacher's reward power has a direct impact on interaction and knowledge sharing behavior though other powers do not.

Matzler, Renzl, Muller, Nerting, and Mooradian (2008) used the framework of Big Five personality dimensions to explore relationships between three personality traits (agreeableness, conscientiousness, and openness to experience) and knowledge sharing among 124 employees of an internationally operating engineering company. The results of the study suggest that agreeableness, conscientiousness, and openness influence knowledge sharing.

Zboralski (2009) used the social theory of learning to look at knowledge sharing in the context of communities of practice (CoPs) among 222 members of multinational companies.

Paroutis and Al Saleh (2009) conducted a qualitative study using grounded theory to study the reasons for and barriers to knowledge sharing and collaboration among 11 employees (5 users of Web 2.0 and 6 nonusers). The study identified four key determinants of knowledge sharing using Web 2.0 technologies: history, outcome expectations, perceived organizational or management support, and trust.

He (2009) used social interdependence theory (Johnson & Johnson, 1987), cognitive development theory (Piaget, 1965), and social constructivist theory (Jonassen, Davidson, Collins, Campbell, & Haag, 1995) to study the relationships between trust, mutual influence, conflict, leadership, cohesion, quality, and quantity of knowledge sharing and students' grades for 148 undergraduate students. Social interdependence theory argues that there must be a type of interaction in which individuals have each other determine the outcomes. Social cognitive theory emphasizes the importance of cognitive conflict for cognitive development. Social constructivist theory emphasizes the importance of collaboration for knowledge construction. The results of the study suggest that mutual influence and team cohesion are major factors affecting knowledge sharing. Conflict mediates the relationship between trust and knowledge sharing. Leadership has a strong relationship with team cohesion, which has a relationship with knowledge sharing. No significant relationship exists between quantity of knowledge sharing and student grades.

Ma and Yuen (2011) used the social interaction theory (Baumeister & Leary, 1995) to study the relationship between perceived online attachment motivation and perceived online relationship commitment to online knowledge sharing behavior for 581 undergraduate students.

Li (2010) used the united theory of acceptance and use of technology (Venkatesh, Morris,Davis, & Davis, 2003) in a qualitative study with 21 American and 20 Chinese employees who worked for a multinational Fortune 100 company. The purpose of the

study was to explore the relationships between organizational factors (performance, expectancy, compatibility based on work practice, knowledge sharing culture, and time pressure), and cultural factors (language, different thinking logic, and different level of perceived credibility for knowledge sharing) and online knowledge sharing. The theory maintains that performance expectancy, effort expectancy, social influence, and facilitating conditions influence use behavior in information systems. The results of the study suggest that performance expectancy, compatibility based on work practice, knowledge sharing culture, and time pressure strongly influence knowledge sharing for both Chinese and Americans. Language, different thinking logic, and different levels of perceived credibility to voluntarily share knowledge showed cultural differences (Chinese participants contributed knowledge less frequently than U.S. peers).

A number of studies (Bock & Kim, 2002; Forstenlechner & Lettice, 2007) used social exchange theory (Blau, 1964) to study knowledge sharing. According to social exchange theory, social interaction originates the expectation that social rewards will follow (Wasko & Faraj, 2005).

Bock and Kim (2002) studied actual knowledge sharing among 467 employees from four large, public organizations. Additionally, the study explored the intention to share. The study concluded that social exchange (nonmonetary) can explain knowledge sharing because it suggests reciprocity of favors, meaning that if an individual receives something from another individual, that person will feel obligated to offer something in return.

The study by Forstenlechner and Lettice (2007) explored the relationship between the means that motivate knowledge sharing (e.g., career prospects, authority, provision of charge codes, recognition among peers, and online incentives) and knowledge sharing and creation in more than one-fourth of the more than 2,500 lawyers in multinational

law firms in more than 25 offices in over 15 countries. The results of the study suggest that the means that motivate knowledge sharing have diverse impacts around the world.

Jeon et al. (2011) studied the relationships between intrinsic and extrinsic motivation and knowledge sharing attitudes, intentions, and behaviors among 282 employees in large Korean high technology production companies. The results of the study suggest that both intrinsic and extrinsic motivation positively influence attitudes towards knowledge sharing behavior, but that intrinsic motivation is more influential. Differences in knowledge sharing mechanisms were noted between formally managed communities of practice and informally nurtured communities of practice.

Hong and Vai (2008) conducted a case study with various cross-functional virtual team members in a local subsidiary of a multinational telecommunication corporation and two of its hardware vendors. The results of the study suggest that team members employ the following four knowledge sharing mechanisms: shared understanding, learning climate, job rotation, and coaching. Among these four, shared understanding and learning climate are able to overcome the unwillingness of virtual team members to participate in the knowledge sharing process; whereas coaching and job rotation compensate for the lack of collective competence required for performing the co-operative works.

Lin, Hung, and Chen (2009) used social cognitive theory (Bandura, 1986, 1997) to study the relationships between contextual factors (e.g., norms of reciprocity, trust), knowledge sharing, and community loyalty for 350 members of three professional virtual communities. The study used knowledge sharing self-efficacy, perceived relative advantage, and perceived compatibility as mediating variables. According to social cognitive theory, there is reciprocal causation between person, environment, and behavior. The results of the study suggest that trust significantly influences knowledge sharing self-efficacy, perceived relative advantage, and perceived compatibility, which

in turn positively affect knowledge sharing behavior. Norms of reciprocity do not significantly affect knowledge sharing behavior.

2.6 Information Security Knowledge Sharing

Information security has become increasingly significant in the business sector today due to the substantial increase in information security threats, and the constant expansion of the procedures and regulations for information security. Companies and institutions expend considerable resources containing threats that threaten their information systems. They apply a collection of anti-spyware/anti-virus software, intrusion detection and prevention systems, firewalls, and content filtering software to secure their information systems. However, human failure and errors may pose many obstacles in the provision of security to an institution.

Generally, information security is recognised to be a technical problem; hence, all the people who handle such problems are technicians. This faulty view about information security leads to negligence pertaining to the human role and associated determinants. Information security experts usually regard the human factor as a vulnerable aspect of the information security mechanism. Negligence of the human factor in information security has become a serious issue upon which numerous descriptive researches (Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2012; Lee & Kozar, 2005) and field studies (Choo, 2011; Potter & Beard, 2010) have focused. Investigation of the human factor and role in the framework of the information security has been the primary focus of much research in recent years. For example, Loch and Conger (1996) studied social criteria and sentimental factors in the moral behaviour of computer users. In their research, they primarily attempted to find strategies to prevent counterproductive behaviour of computer users in information security. The most important finding in their research is that the human factor or agents may have mischievous motives. Therefore, there must be an extrinsic pre-emptive force, such as

punishment, to control such motives. Although considerable research has been conducted on how to prevent the bad and troublesome behaviour of end users, there has been very little research concerning how to elicit good and proper behaviour among end users in information security (Feledi & Fenz, 2012; Stanton, Stam, Mastrangelo, & Jolton, 2005). Knowledge sharing is good behaviour, which can be defined as the attitude of a user to distribute his/her obtained knowledge to the other participants within a community (Bock & Kim, 2003). Hung and Cheng (2012) contended that knowledge sharing should be considered as a process, an action or a behavior. Ryu, Ho and Han (2003) put forward another definition for knowledge sharing. They defined knowledge sharing as a connecting behavior in which people try to gain knowledge from others. Meanwhile, Lee (2001) defines knowledge sharing as the willingness of individuals, groups or institutions to convey or spread knowledge to others. Holthouse (1998) maintained that knowledge is a flow concept and that knowledge holders share their knowledge with knowledge receivers. Furthermore, Bock, Zmud, Kim and Lee (2005) defined knowledge sharing as the attitude of individuals to construct and transfer knowledge whereas Wijnhoven (1998) maintained that knowledge conveyance occurs via information media in which recipients are able to add new knowledge to their existent knowledge. The emergence of the Internet has popularized interaction and information sharing among users via virtual space or cyberspace. Yang and Maxwell (2011) identified different factors influencing knowledge sharing from three perspectives: interpersonal, intra-organizational, and inter-organizational. Knowledge sharing in virtual space is mostly related to the interpersonal perspective. Users from all walks of life join virtual communities in order to share their knowledge relevant to common interests and topics. In fact, cyberspace communities work as warehouse of knowledge that provides people with an opportunity to receive or share information. NIST Special Publication 800-137(Dempsey, 2011) pointed out that knowledge sharing

promotes collaboration and cooperation among organizational entities; facilitates sharing of security-related information; provides an organization-wide forum to consider all sources of risk; and ensures that risk information is considered for continuous monitoring decisions.

Sharing of information and experience amid information security professionals decreases risk (Tamjidyamcholo & Al-Dabbagh, 2012), and, significantly, saves investment in information security (Liu, Ji, & Mookerjee, 2011). Furthermore, sharing Knowledge among information security technicians can restrain an independent person from reaching a similar solution; above all, knowledge sharing can generate outstanding solutions for the problems (Feledi & Fenz, 2012). Moreover, Ma and Yuen (2011) put forward that the success of online learning depends on knowledge sharing process. Currently, virtual space is a common and joint environment in which experts are able to find each other and share their knowledge and information (Lin, Lin & Huang, 2008).

2.7 Virtual Communities and Professional Virtual Communities

There is difference between virtual communities and professional virtual communites.

2.7.1 Virtual Communities

Earlier literature associated with communities mentioned two forms of social groups. The identified social groups are communities and societies or associations (Tonnies, 1955). Tonnies pointed out where the regular membership of the group relates to a particular objective that associations are characterised as groups. Structured and formal are important elements that explain the relationship within the association. On the other hand, a community is spelled out as having members who make intense and personal relationships. A sense of identity is created among individuals within these kinds of relationships. A virtual community is actually defined by Barab, Makinster, and

Scheckler (2003) as “a persistent, sustained social network of individuals who share and develop an overlapping knowledge base, set of beliefs, values, history, and experience focused on a common practice and or mutual enterprise”. With growing of the Internet as well as Web 2.0, social networks are tending to make a substantial effect on online communities becoming ones themselves.

The net has result in an expansion of virtual communities all around the world (Fernback, 1999). Horrigan along with Rainie (2006) suggested that the achievement of the Internet is due to connecting individuals to share knowledge, understanding, and advice. In 2005, additionally they noted that around 53 million adult people utilized a virtual community to make decisions regarding their own life. In today’s world, our lives are drastically influenced by knowledge and information sharing within VCs (Lin, Hung & Chen, 2009). Lee et al. (2002) scrutinized a number of studies relating to virtual communities and have proposed four main features for a virtual community. These features include that (1) a virtual community must be constructed based upon a computer-mediated space, which is labeled cyberspace; (2) information technology is the major driving force, which makes virtual community activities possible; (3) participants of a virtual community are the only ones who determine the topics and contents of a virtual community; and (4) contacts among virtual community members promote the relationships within a virtual community. Accordingly, they put forward an operational definition for a virtual community. A virtual community is a technology-oriented cyberspace, which is based upon the connections and communications of its members, and is able to create a relationship.

2.7.2 Professional Virtual Communities

Professional or technical communities are different from general communities in several aspects. A significant achievement of professional virtual communities is to offer

resolution, novel insight, and frameworks in knowledge sharing and management for institutions (Chen & Hung, 2010). Participants attend PVCs in order to maintain knowledge security, solve problems, increase their expertise, obtain more technical knowledge and propose more innovations. PVCs are highly regarded by many institutions as an effective tool in their knowledge management activities. These organizations have taken major strides to develop and expand such communities (Gongla & Rizzuto, 2001). Bifulco and Santoro (2005) defined the Professional Virtual Community as a human-centric business entity that has been built to improve the realization of knowledge workers and also to best assist creativity cycles inside the associated socio-economic surroundings .

The PVC can be a connection of people recognized by a particular knowledge scope by having explicit business orientation which targeted at producing value via members' collaboration, sharing and interaction. This particular interaction amongst the members is optimized through face-to-face mechanisms and the synergic utilization of ICT mediated (Bifulco & Santoro, 2005).

Santoro and Bifulco (2008) pointed out that the PVC created value including:

• Developing and enhancing knowledge for example the creation of novel knowledge associate with the community knowledge scope

• Providing professional services such as the collaborative business activities carried out through the members exploiting the community knowledge

• Creating social cohesion for instance, the social connections between the members that make it possible for their cooperation readiness - specifically promote knowledge sharing and co-creation - and the time and effort reduction to begin collaboration.

The epiphenomenon of the individual cohesion recognized within the PVC would be the creation of larger practical capabilities which is often termed as "collective intelligence".

A professional or technician is defined as a person who has technical knowledge and problem-solving capabilities about a specific area of expertise, shows commitment toward his/her job, and improves his/her capabilities via critical reflection. By and large, occupations like teachers, specialists, lawyers, physicians, and consultants are regarded as professionals (Chen, 2007). We can define a professional virtual community as an expanded community with a shared activity (Wenger, 1998). According to Hagel's categorization (1999), a professional virtual community is viewed as a virtual community with common interest. Such community gathers a scattered group of people together with shared expertise and knowledge about a particular area. Bressler and Grantham (2000) assert that PVC attracts individuals with similar and common interests who cooperate with each other in order to accomplish common goals. Participants of a professional virtual community engage in community activities overtly rather than covertly or anonymously (Klang & Olsson, 1999). It is also possible for community members to interact and communicate with others as groups (Cowan, Mayfield, Tompa & Gasparini, 1998). TappedIn (http://www.tappedin.org), TENet (http://www.tenet.edu), and SCTNet (http://sctnet.edu.tw) can be examples of PVCs. Hung and Cheng (2012) pointed out that the usage of the PVCs is currently a hot topic and needs further research to be conducted in this environment.

Santoro and Bifulco (2008) mentioned that PVCs as a new organizational arrangement in European industry emerged in order to address two objectives:

- to increase the European Industrial competitiveness
- to enhance the Knowledge workers' quality of life

The general principle ruling the PVC members' participation is that it is up to the members to decide the type and the extent of their individual involvement in the community activities, which is complementary to and co-existent with their normal working occupational forms (Tamjidyamcholo et al., 2013). The PVC members are not

PVC employees. The PVC members can be individual professionals, free-lances, company employees, researchers (from university or research centres), retired knowledge workers, and even common people (Bifulco & Santoro, 2005). The PVC composition depends on its specific typology and on the socio-economic environment in which the PVC is established.

2.8 Summary of Literature Review

In the early days of information technology (IT), corporation used IT systems to gain competitive advantages to their competitors because setting up a competitive business technique, model, or method allowed an organization to provide service or product which is superior and creates a competitive advantage. Nowadays, almost all of the organizations using IT systems, therefore and it cannot be a competitive advantage. However, if the organizations cannot provide security for their IT systems, advantages may replace by disadvantages and result to lose market share. Safe environment must design and generate that organizations can keep up with the competition in which procedures and business process can function safely. Providing security of all components for organizations is difficult. They only can be managed under umbrella of information security risk management. The ISRM is identifying vulnerabilities in organization's assets and taking reasoned steps to ensure the integrity, confidentiality and availability of all the components in the organization's information system. Risk management analyses possible incidents and possible consequences before happening to keep risk an acceptable level. There are different models for the ISRM, such as: NIST 500-30, ISO/IEC 27005, OCTAVE, and Microsoft. The models in the main steps are the same; however in some aspects they are different. Based on ISO/IEC 27005, risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, knowledge sharing, risk monitoring and review. Knowledge sharing is

an important component of the ISRM process. Security knowledge sharing substantially reduces investment in information security.

The emergence of the Internet has popularized interaction and information sharing among users via virtual space or cyberspace. Users from all walks of life join virtual communities in order to share their knowledge that are relevant to common interests and topics. In fact, cyberspace communities work as a warehouse of knowledge that provides people with an opportunity to receive or share information. The evaluation of the virtual communities in information security has shown that, the most important challenge for knowledge sharing is motivating users to participate in knowledge sharing activity. However, many professional virtual communities have failed due to reasons, such as the low willingness of members to share knowledge with other members. Hence, the academic goal of this study is to gain insights on the determinants that directly influence on information security professionals' decision to share his or her knowledge in professional virtual communities. In addition, it is to find relationship between knowledge sharing behaviour and information security risk

CHAPTER 3

RESEARCH MODELS AND HYPOTHESES

3.1 Introduction

This research proposes two models to understand and determine the determinants of knowledge sharing behavior in information security PVCs. First model analyses key determinants, containing attitude, self-efficacy, trust, norm of reciprocity, and shared language, in respect of the information security workers intention to share knowledge. Second model is composed of two main parts. The first part is the Triandis theory, which is adapted to understand the other determinants of knowledge sharing behavior in information security PVCs. The second part explores the quantitative relationship between knowledge sharing and security risk reduction. The present chapter comprises the following sections. The next section presents hypothesis development and conceptual model for first research model. In Section 2, the hypothesis development and conceptual model of second research model is presented. Section 3, summarizes the content of this chapter.

3.2 Hypothesis Development of First Research Model

Background of hypotheses and their theory for the first proposed model is presented in the following subsections.

3.2.1 Theory of Reasoned Action and Knowledge Sharing

The theory of reasoned action **(**TRA) is known as a broadly accepted model to study various types of behaviour (Ajzen, 2006; Fishbein & Ajzen, 1975). According to the TRA, intent can truly predict behaviour. The TRA puts forward the idea that human behaviour is thoroughly logical, and that it applies limited information, which is at an individual's disposal. Behavioural intention can accurately predict a behaviour, and it

can be used to determine the relative strength of a person's intention to undertake an action and demonstrate a behaviour.

Attitude is intertwined with intention, and determines a person's intention (Ajzen, 2006; Hsu & Lin, 2008). Attitude can be defined as a person's inclination to react to an object or an idea in a positive or negative way (Chen, Chuang, & Chen, 2012). In knowledge sharing activities, attitude has been proven to be a significant factor because what a person knows about solving problems can affect his/her trade value (Fishbein & Ajzen, 1975). When the employees of a company find that knowledge sharing is very important and beneficial for their company, they will voluntarily engage in knowledge sharing activities. On the other hand, if a person loses power or assets in knowledge sharing or knowledge producing, they will restrain from sharing their personal knowledge with competitors (Hsu & Lin, 2008).

A person's attitude towards a behaviour can accurately predict their intention for engaging in that behaviour. Accordingly, a person's attitude towards knowledge sharing determines his/her behavioural intention for sharing knowledge (Chow & Chan, 2008). This approach is used to generate the first hypotheses of the present study.

H1. Attitude to sharing knowledge positively affects an individual’s knowledge sharing intention.

3.2.2 Role of Self-efficacy in Knowledge Sharing

In information systems (IS) research, the social cognitive theory (Bandura, 1986) has been predominantly employed. This theory is found to have much credit and validity. Two fundamental factors that have much significance in this theory and are believed to have a substantial influence on human functioning are outcome expectations and self-efficacy. Outcome expectation is “a judgment of the likely consequences that will be

produced by performance", whereas self-efficacy is "a judgment of one's ability to organize and execute given types of performance" (Bandura, 1997).

In recent years, several studies have drawn upon the social cognitive theory and have investigated the relationship between personal cognition – for example outcome expectations and/or self-efficacy – and computer usage and Internet behaviour (Hsu, Ju, Yen & Chang, 2007; Luarn & Lin, 2005). Outcome expectation is excluded in the present model, since we want to increase validity of our instrument in data collection process. In the second model of this thesis the outcome expectation is investigated.

Self-efficacy is a sort of self-assessment, which plays a crucial role in determining a person's behaviour (Bandura, 1986). A high level of self-efficacy in a person will make them much more self-confident about their abilities and skills, and it strengthens motivation. Therefore, such a person will engage in actions and activities more enthusiastically and employ their cognitive resources to successfully perform a duty (Bandura, 1997). Self-efficacy increases one's endeavours and efforts, self-regulation, and the persistence and perseverance of an individual when they are confronted with a challenge and barrier (Bandura, 1986). Various researchers have empirically confirmed this concept (Tsai & Cheng, 2010; Chen, Chuang, & Chen, 2012). Accordingly, the following hypotheses are assumed:

H2a. An individual's self-efficacy is positively associated with their intention towards knowledge sharing.

H2b. An individual's self-efficacy is positively associated with their attitude towards knowledge sharing.

3.2.3 Effect of Trust on Knowledge Sharing

In management jargon, trust refers to what an individual thinks about the integrity, capability and compassion of another person (Gefen, Karahanna & Straub, 2003). The focus of the present study is on integrity. Integrity alludes to an individual's anticipation about other users of a virtual community – whether or not they comply with ethics, criteria and principles that are broadly accepted. According to IS, group cohesiveness and performance (Huang, 2009), organizational value creation (Tsai & Ghoshal, 1998), individual motivation on knowledge sharing (Chang & Chuang, 2011), online transactions (Chang, Cheung & Lai, 2005), and knowledge sharing behaviour (Lin, Wu, & Lu, 2012), trust is an essential prerequisite. Nahapiet and Ghoshal (1998) maintain that trust can make two parties involved in a virtual interaction more zealous and enthusiastic to cooperate. Nonaka's (1994) study demonstrates that trust between individuals plays a substantially important role in an organization and teamwork. When people are involved in a casual relationship, it is very difficult to evaluate their attitude towards that relationship. This is a noticeable characteristic of casual and informal inter-connections (Bartol & Srivastava, 2002). Therefore, trust appears to be much more significant in voluntary activities, such as knowledge sharing in a virtual community (Kim & Ahmad, 2012; Zolfaghar & Aghaie, 2012). Blau (1964) asserts that trust can construct and maintain the exchange of ideas in an interconnection, and, ultimately, it will end up in sharing excellent knowledge.

With regard to previous studies about trust development, we have applied three trust determinants in knowledge sharing: Information-based trust, Identification-based trust, and Content-based trust.

(i) Information-based trust, which is also known as knowledge-based trust (Lander, Purvis, McCray & Leigh, 2004; Panteli & Sockalingam, 2005), is built when two

parties involved in an interaction know each other well. Hence, they can predict each other's behaviour and their suspicion of each other will decrease considerably. As its name denotes, information-based trust is built upon information (Ba, 2001). It does not arise from pursuing the rewards of truthfulness or fearing a penalty (Lander, Purvis, McCray & Leigh, 2004). Ratnasingam and Pavlou (2002) contend that information-based trust will evolve between businessmen because they have to comply with technical criteria, insurance and protection policies and security strategies. In addition, Ratnasingam (2005) illustrates that information-based trust can be defined as an abstract expectation according to which basic control tools and technological infrastructure are able to foster trade and business. Therefore, in the present study, information-based trust can be specifically defined as the degree of trust the users of PVCs have in it with regard to the technological mechanism and proper privacy of the PVC.

(ii) Identification-based trust, which is also known as transference-based trust (Ba, 2001), will evolve between two individuals when they truly respect and perceive each other's desires. They can understand and appreciate each other, and this reciprocal understanding can reach the point where they are willing to do everything on behalf of the other (Lander, Purvis, McCray & Leigh, 2004). When people are able to relate to others emotionally, identification-based trust will evolve. People are passionate and emotional about the relationships in which they have trust. They care for the well-being of other partners and are willing to help; they seek internal satisfaction and fulfilment in such relationships and they are thoroughly convinced that these sentiments are totally mutual (McAllister, 1995). In doing so, they can achieve a collective identity and a healthy and robust inter-connection, which will definitely encourage them to cooperate with each other and build collective capabilities and strength (Panteli & Sockalingam, 2005). Accordingly, in the present study, identification-based trust is specifically

defined as users' trust in PVCs, which originates from sentimental inter-connection between participants.

(iii) Content-based trust, which is also known as knowledge quality trust (Hsu, Ju, Yen & Chang, 2007), is built upon the values and merits of knowledge that are being distributed in a virtual community (Chang & Chuang, 2011). It seems that safety and security technicians are more worried about the merits and values and nature of shared knowledge in VCs. Therefore, in the present study, content-based trust is specifically defined as users' trust in PVCs, which originates from the merits and values and content of shared knowledge between users.

It is very important to realize the attitudes and intent of security technicians in PVCs and trust can be beneficial in achieving this goal. Therefore, hypotheses 3a and 3b are as follows:

H3a. Trust is positively associated with the individual's intention of knowledge sharing.

H3b. Trust is positively associated with the individual's attitude to knowledge sharing.

3.2.4 Effect of Norm of Reciprocity on Knowledge Sharing

In the present research, norm of reciprocity is defined as the exchange of information and knowledge, which is mutual and fair. In other words, both parties involved in this relationship consider this exchange of knowledge as fair and just. Blaua (1964) maintains that norm of reciprocity signifies "actions that are contingent on rewarding reactions from others, and that cease when these expected reactions are not forthcoming". The social exchange theory (Thibaut & Kelley, 1959) puts forward the idea that users of a virtual community seek a shared reciprocity from other members.

This kind of reciprocity will justify the time and attempts they have spent on knowledge sharing. Davenport and Pruzak (2000) introduce the notion of the knowledge market

and assert that reciprocity is a crucial factor that impels knowledge sharing. It has been demonstrated by previous researchers that when knowledge sharing is accompanied by an intense sensation of reciprocity, it can enhance the activities and performance of electronic networks remarkably (Wasko & Faraj, 2005). Thus, the hypotheses are:

H4a. Norm of reciprocity is positively associated with the individual's intention of knowledge sharing.

H4b. Norm of reciprocity is positively associated with the individual's attitude to knowledge sharing.

3.2.5 Role of Shared Language in Knowledge Sharing

A shared language encompasses concepts and ideas, which are broader than the language itself. It deals with "the acronyms, subtleties, and underlying assumptions that are the staples of day-to-day interactions" (Lesser & Storck, 2001). A shared language and codes play an important role in eliciting appropriate behaviour and actions and help a virtual community's participants understand the shared goals of that community (Tsai & Ghoshal, 1998). Nahapiet and Ghoshal (1998) propose that a shared language can affect the necessary conditions for the exchange and integration of intellectual assets and capital in different fashions. Firstly, a shared language helps people get in contact with others and gain knowledge and information from them. Secondly, a shared language can create a theoretical framework for participants to evaluate the probable merits of integration and exchange of knowledge. Finally, a shared language generates an overlap in knowledge. Therefore, a shared language can increase the ability of participants to integrate the pieces of information they have gathered through social contacts and connections. In a virtual community, participants do need a shared language for learning (Nahapiet & Ghoshal, 1998). A shared language helps participants to create a shared jargon and vocabulary in the community to connect with

each other. In doing so, a shared language provides a common ground to share thoughts and ideas, and also facilitates communication among participants who have practical experience and a similar background. Thus, a shared language will encourage participants to voluntarily and enthusiastically engage in knowledge sharing actions and promote the whole process of knowledge sharing. Therefore, hypothesis 5a and 5b are proposed based upon this concept:

H5a. A shared language is positively associated with the individual's intention of knowledge sharing

H5b. A shared language is positively associated with the individual's attitude to knowledge sharing.

3.3 First Research Model

Figure 3.1 depicts the theory development and conceptual model of the present study. This model is based upon the aforementioned discussion and concepts. It explains the relationship between self-efficacy, trust, norm of reciprocity and shared language with knowledge sharing attitude. It shows that these factors will, directly or indirectly, develop knowledge sharing attitude and influence the intentions of participants to engage in knowledge sharing activities. With regard to this model, nine hypotheses have been examined. Each hypothesis is depicted by H, an alphanumeric and a number. The plus symbol shows a positive relationship whereas the arrows show the hypothesized relationship.

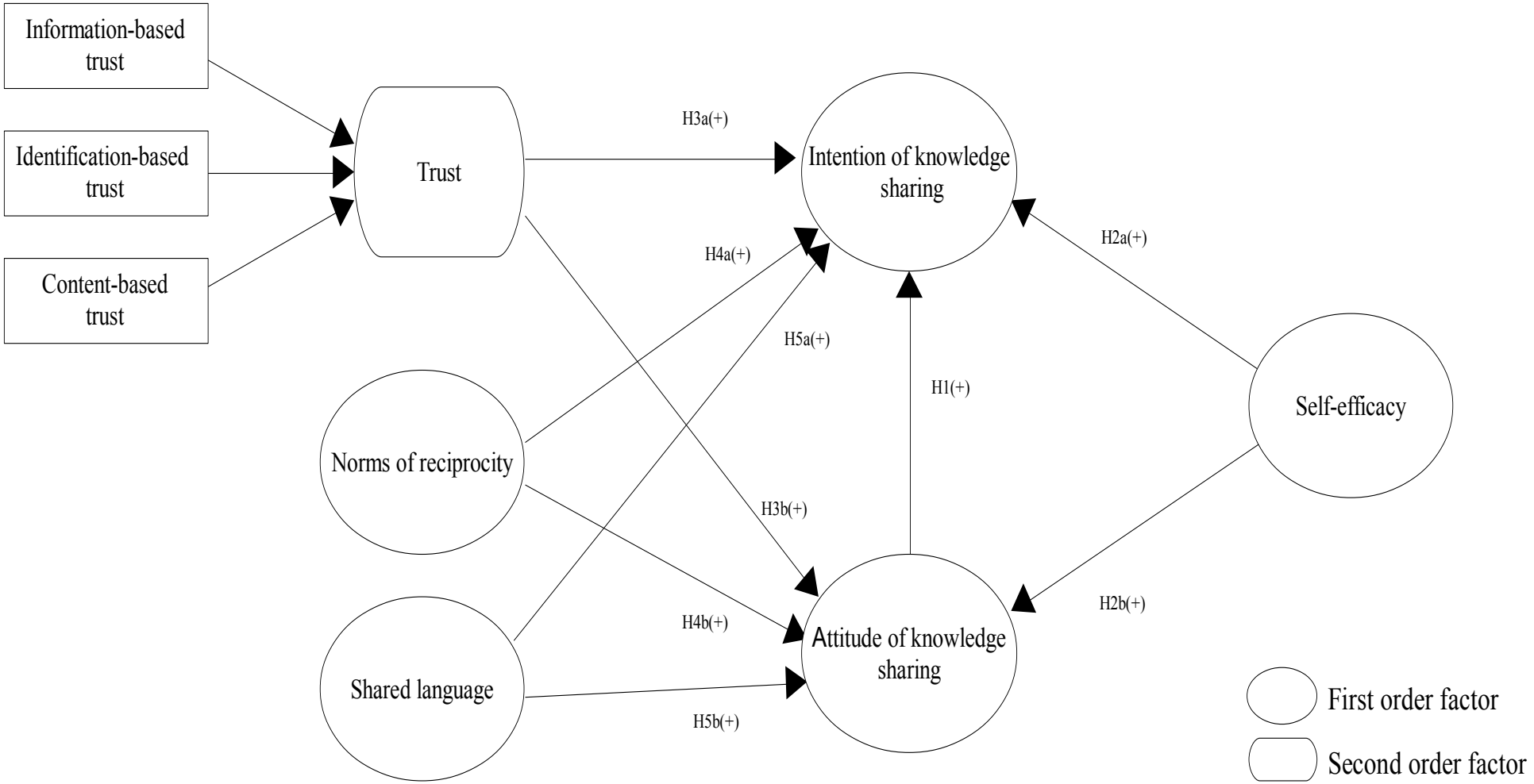

Figure 3.1 First Research Model

3.4 Hypothesis Development of Second Research Model

Background of hypotheses and their theory for the second proposed model is presented in the following subsections.

3.4.1 Triandis Theory and Knowledge Sharing

Ajzen and Fishbein's (1980) model of beliefs, attitudes and behavior is regarded as a reference model by many information system researchers in order to elucidate the knowledge sharing behavior of users (He & Wei, 2009; Kuo & Young, 2008). Nevertheless, however instrumental this model seems to be, it is still an incomplete model since it puts aside determinants that may affect behavioral intentions and behavior itself (Triandis, 1979). Triandis (1980) introduced an exhaustive model for interpersonal behavior in order to cover a broader range of related determinants. This model comprises a wide range of determinants and hypotheses. The present study has only applied a subset of the Triandis model; hence, it does not seem necessary to discuss this model and its 34 relevant hypotheses in detail here. For a thorough discussion of the model, the reader should refer to Triandis (1979). The core idea of this model is that perceived consequences, affect, and social factors affect the behavioral intentions of individuals, and, in turn, these intentions affect behavior. According to Triandis (1979), behavior itself is directly and indirectly influenced by habits. He further contends that the expected behavior would not happen even when there is a high degree of motivation and intention if the facilitating conditions impede the occurrence of the behavior. Thus, if someone intends to use a virtual community but does not have easy access to one, usage is less likely to occur. In the present study, a subset of the Triandis theory (1980) is examined with regard to the knowledge sharing attitude of information security specialists within PVCs. In particular, the direct impact of perceived consequences, affect, social factors and facilitating conditions on the behavior

have been studied. Behavioral intention was set aside from the model as had been done in other similar studies (Thompson, Higgins, & Howell, 1991; Bergeron, Raymond, Rivard & Gara, 1995; Cheung, Chang & Lai, 2000; Jeon, Kim & Koh, 2011) since the focus of the study is the genuine behavior (i.e. participation in PVCs). Similarly, habits were also put aside from the model as had been done in other similar studies (Thompson, Higgins & Howell, 1991; Bergeron, et al., 1995; Cheung, Chang & Lai, 2000; Jeon, Kim & Koh 2011), since habits (i.e. former uses), in the context of participation in PVCs, exhibited a tautological relationship with the present usage.

The Triandis model has been shown to be instrumental in illustrating and forecasting a wide range of intentions, such as mammography usage, work-out intention and behavior, and inclination to get involved in casual sex (Triandis, 1979). Furthermore, the Triandis model has been used to study IS usage. This model has been applied in two studies regarding the usage behavior of individuals of personal computers (Thompson, Higgins & Howell, 1991). Pare and Elam (1995) also implemented this model to scrutinize the usage behavior of personal computers. In addition, this theory has been widely used to study the executive behavior of EIS (executive information system) usage (Bergeron, Raymond, Rivard & Gara, 1995). Another study scrutinized the relationship between the behavior of end-users and their PC usage among knowledge workers in Saudi Arabia (Al-Khaldi & Olusegun Wallace, 1999). Cheung, Chang, and Lai (2000) conducted a research investigating different factors that influence Internet/WWW usage in the working environment. Cheung, Chang, and Lai (2000) performed a confirmatory study to identify the motivation and intention of using the Internet/WWW at work. The Triandis model has also been applied to discern inter-organizational knowledge sharing factors that may have an impact on the knowledge sharing activities of community members (Jeon, Kim & Koh, 2011). In general, the Triandis model has been broadly utilized in a wide range of studies relating to

information systems. The fundamental and related constructs of the present study model will be discussed in more detail in the following sections.

3.4.2 Perceived Consequences

According to Triandis (1971), a crucial determinant that could influence behavior is the expected consequences of behavior, later renamed perceived consequences (Triandis, 1980). The perceived consequences construct is based upon the expectancy theory of motivation, which was put forward by Vroom (1964). This theory was further evolved by Porter and Lawler (1968). The factor “consequences" lie in the expected value of behavior. This is known as a function of the perceived consequences of an action and the value of each consequence. Perceived consequence is defined as the possibility that a specific consequence would occur as a result of behavior. Bergeron, Raymond, Rivard and Gara (1995) contended that as the expected value of an action increases, an individual will be more willing to engage in that action. Jeon, Kim and Koh (2011) proclaimed that when perceived consequences have high strength and intensity, the extent and prevalence of knowledge sharing will increase. Perceived consequences are believed to have many dimensions. Triandis (1971) acknowledged that the perceived consequences construct of his model is not unidimensional, but probably comprises several components. This fact is in agreement with the theoretical discussions and experimental results of other studies; proposing that perceived consequences have multiple dimensions (Azjen & Fishbein, 1980; Lucas, 1978; Schultz & Slevin, 1973). Prior studies that applied the Triandis model to the information technology acceptance context, in general, defined the perceived consequences as consisting of near-term consequences, long-term consequences, and complexity (Al-Khaldi & Olusegun Wallace, 1999; Cheung, Chang, & Lai, 2000). In addition, Jeon, Kim and Koh (2011) introduced new sub-dimensions for the perceived consequences construct including

organization-member, member-member, and member-work to encompass knowledge sharing activities of the community. However, with respect to knowledge management and the virtual community literature, the perceived consequences are defined as a construct consisting of expected usefulness, expected social interaction, and expected reputation in the present study.

3.4.2.1 Usefulness

Whether a person is willing to share knowledge or not is influenced by the perceived gains he/she may achieve and the cost this decision may bring about for them. Anticipated usefulness is the positive outcome that members of communities expect to see in their work as a result of their knowledge sharing. This is similar to the construct of perceived usefulness (PU) in the Technology Acceptance Model (Davis, Bagozzi & Warshaw 1989). Hu, Clark and Ma (2003) found that there is a significant and eminent relationship between job relevance, perceived usefulness and information technology acceptance. A professional community is a community with shared and common activities; therefore, it is quite reasonable to see every member of the community believing that the actions of the VC would result in better work performance. Wenger (1998) demonstrated that community members are able to enhance their work performance via knowledge sharing. Perceived usefulness of community was believed to encourage knowledge sharing in VCs within the virtual community framework (Wasko & Faraj, 2005). Typically, expected usefulness – the beliefs regarding useful consequences of knowledge sharing – has been defined as a crucial determinant to forecast knowledge sharing behavior in previous empirical studies on knowledge sharing (Hult , Ketchen & Nichols 2002; Bock et al., 2005; Kankanhalli et al., 2005; Wasko & Faraj, 2005).

3.4.2.2 Social Interaction

Social interaction ties (network ties) are described as pathways for the flow of information and resources (Tsai & Ghoshal, 1998). Granovetter (1973) believed that tie strength is composed of time period, sentimental intensity, intimacy (reciprocal confiding) and mutual services, which typify a tie. In the present study, social interaction is defined as the intensity of relationship, the time period passed, and the extent of connection occurrence among virtual community members. Nahapiet and Ghoshal (1998) contended that "the fundamental proposition of the Social Capital Theory is that network ties provide access to resources" (p. 252). Larson (1992), and Ring and Van de Ven (1994) observed that as connecting or exchange parties engage in more social interaction, the strength, the rate of occurrence, and the prevalence of information increase. In fact, knowledge is an essential prerequisite for an action; however, it is hard and expensive to achieve. Members of a virtual community are able to have access to diverse and numerous sources of knowledge via social interaction. It is known as a cost-effective tool to share knowledge. Nahapiet and Ghoshal (1998) asserted that "network ties influence both access to parties for combining and exchanging knowledge and anticipation of value through such exchange" (p. 252). In addition, it will be viable to integrate and share knowledge through social interaction. Recent studies have provided empirical support for the influences of social interaction on the quality and quantity of the shared knowledge (Chang & Chuang, 2011), knowledge sharing among units that compete with each other for market share (Tsai, 2002), and group cohesiveness (Huang, 2009).

3.4.2.3 Reputation

Knowledge contributors are able to gain more profit when they have the chance to show others that they have invaluable skills and capabilities. In doing so, they will boost their

self-image and will be considered as experts or scholars, and build a reputation for themselves (Ba, Stallaert & Whinston, 2001). Accordingly, such personal gains will become the core motivation for members to engage in knowledge sharing (Kankanhalli, Tan & Wei, 2005). Reputation is acknowledged as a perceived consequence or gain that urges individuals to share knowledge in virtual communities. Reputation will empower individuals to achieve and keep their status in a community (Marett & Joshi, 2009) and prevent the retention of free riders who do not contribute to the team effort. It is shown by a number of studies that individuals engage in knowledge management activities because they think they will be able to build a reputation for themselves and improve it (Donath, 1999; Wasko & Faraj, 2005) or obtain peer recognition (Carrillo et al., 2004). Consequently, individuals who believe knowledge sharing could raise their reputation will be more inclined to share knowledge (Ba et al., 2001; Wasko & Faraj, 2005). The findings of recent empirical studies affirm that reputation plays a vitally important role in a contributor's willingness and the extent of his/her contribution (Wasko & Faraj, 2005). Therefore, it can be concluded that building reputation and improving status are among the significant factors that can motivate the members of PVCs to engage in knowledge and content sharing via more recurrent and smart responses.

For an understanding of the members of PVCs, the perceived consequences resulting from knowledge sharing in terms of expected usefulness, expected social interaction, and expected reputation dimensions lead us to the first hypothesis.

Hypothesis 1. The perceived consequence is positively related to the knowledge sharing behavior of members in PVCs.

3.4.3 Affect

Affect is described as an individual's feeling of thrill, dissatisfaction, joy, happiness or hatred toward a specific behavior. Positive sentiments intensify the motivation to display a specific behavior, whereas negative sentiments reduce the motivation drive. According to the Triandis model (1980), there is a positive relationship between behavior and affect. In other words, when the thrill and pleasure of behavior is high, it is more likely to occur. Existing findings relating affect to usage in information systems were mixed. Pare and Elam (1995) conducted research on the utilization of personal computers (PCs). The findings of their study show a negative relationship between affect and the usage of PCs. The results of other related studies do not demonstrate a significant relationship between PC usage and affect (Thompson et al., 1991, Cheung et al., 2000). In an attempt to elucidate their insignificant results, Thompson et al. asserted that it might be because PC usage could not evoke a robust emotional reaction. Nonetheless, the reliability measurement rate they have found for the affect construct is very low (Cronbach's Alpha = 0.61), and it may diminish in contact with other determinants. Meanwhile, pleasure and enjoyment, which is considered a construct like affect, is shown to possess a positive relationship with PCs (Igbaria, Iivari & Maragahh, 1995) and usage of the Internet (Teo, Lim & Lai, 1999). Additionally, it is found that affect can play an important role in forecasting other behavior, such as EIS utilization (Bergeron et al., 1995), Internet usage (Chang & Cheung, 2001), and knowledge sharing of CoPs (Jeon et al., 2011). Thus, it is reasonable to hypothesize here that there will be a positive relationship between affect and participation in PVCs.

Hypothesis 2. The affect is positively related to the knowledge sharing behavior of members in PVCs.

3.4.4 Social Factors

According to Triandis (1979), social norms have a direct effect on behavior, and this relationship is dependent on the messages people get from others. It notifies them what to do. Triandis (1980) elucidated further on this topic and proposed the term 'social factors' for this relationship; asserting "the individual's internalization of the reference groups' subjective culture, and specific interpersonal agreements that the individual has made with others, in specific social situations". Subjective culture consists of ways of categorizing experiences, beliefs, attitudes, ideals, roles, norms, and values, which can be understood as the characteristic way that a human group views the human-made part of its environment. Social factors act like the subjective norm in the reasoned action theory (TRA) (Azjen & Fishbein, 1980). Azjen and Fishbein together with Triandis believed that social norms would have a significant effect on behavior. In the present context, it refers to the influence of the security specialists (peers, superior, subordinates) upon his or her use of information security PVCs. The findings of several studies have provided empirical evidence for the relationship between social factors and behavior. For instance, Thompson et al (1991), and Al-Khaldi and Olusegun Wallace (1999) studied the effects of social factors on the usage of PCs among knowledge workers in Canada and Saudi Arabia. The results of their study demonstrate that social factors have a significant influence on the PC usage of participants in both countries. Bock et al. (2005), applying the TRA model, demonstrated that social factors would have a positive impact on the intentional behavior of individuals toward knowledge sharing. Furthermore, Lam (2000) argued that organizational CoPs can create the collective form of knowledge by shared norms embedded in the organizational culture. With respect to the theory of Triandis (1980) and the empirical findings supporting it, the next hypothesis that should be tested is:

Hypothesis 3. The social factor is positively related to the knowledge sharing behavior of members in PVCs.

3.4.5 Facilitating Conditions

Triandis believed that there is a positive relationship between behavior and facilitating conditions. Facilitating conditions are usually regarded as a driving force for users within the context of personal use of information technologies (Bergeron et al., 1995). The present study applies this view as a reference view. Triandis alluded that one might encounter an individual who wants to do something but cannot make it happen because there might be a geographic obstacle that impedes that action. Thus, Triandis added a new construct to his model, facilitating conditions, to forecast behavior. Triandis (1980) offered a definition for these conditions; stating "objective factors, out there in the environment, that several judges or observers can agree make an act easy to do". In the context of our study, the facilitating conditions include guidance; instructions that allow individuals to access the professional virtual community when they want to, as well as the support provided by the community provider to facilitate the use of the PVCs. Past findings on the relationship between facilitating conditions and behavior were supported. The results of previous related studies confirm that there exists a relationship between facilitating conditions and behavior (Chang & Cheung, 2001). Cheung, Chang and Lai (2000) found that the facilitating conditions are the most important determinant of Internet/WWW usage. Jeon, Kim and Koh (2011) found that for more active knowledge sharing within CoPs, the facilitating factors play a significant role. However, cultivating knowledge sharing communities without proper facilitating conditions can give rise to unexpected negative consequences, since the communities are vulnerable (Garud & Kunaraswamy, 2005). Thus we develop the following hypothesis

Hypothesis 4. The facilitating condition is positively related to the knowledge sharing behavior of members in PVCs.

3.4.6 Knowledge Sharing and Information Security Risk Reduction

The PVCs of information security are places that security experts participate and communicate with each other in order to improve their professional learning process (Tamjidyamcholo et al., 2013; 2012). Finin et al. (2009) pointed out that the basic cornerstone of traditional or conventional information security frameworks is "need to know". However, there is a shift towards "need to share" in modern information security frameworks. Kagal, Finin and Joshi (2001) claimed that there are serious attacks against us and we have to create a framework to share our knowledge in order to prevent a catastrophe. Emergence and development of programs like security awareness and training are the result of the need to have security knowledge (Kesh & Ratnasingam, 2007). Some experts have gone further and have suggested that IT specialists should participate in hacker conferences to obtain security knowledge (Conti, 2005). A project has been performed by the multi university research initiative (MURI) to create a secure web-based information sharing community (Finin et al., 2009). There will be a large number of advantages for security experts when they are able to share their knowledge. Therefore, there will not be similar and identical solutions coming from various independent experts, and it will help save invaluable resources that can be utilized more effectively and constructively. In addition, solutions that are created via knowledge sharing would be of higher quality because it will be possible to enhance and complement existent solutions rather than propose similar solutions repeatedly. Feledi, Fenz and Lechner (2013) and Tamjidyamcholo et al. (2012, 2013) drew attention to the fact that knowledge sharing in the information security sector would lead to risk reduction.

In spite of the advantages of information security knowledge sharing, it may create risk to the participants of the community (Kagal, Finin & Joshi, 2003). The users of VCs are becoming more vulnerable to security threats due to the use of information communication technologies (Furnell, Bryant & Phippen, 2007). As an evolving tool, the Internet's dynamic status continues to pose new risks and vulnerabilities. These ever-changing risks and vulnerabilities are being exploited through ignorance, inexperience or people with malicious intent (Lichtenstein, 1998). The risks are classified according to the function of what is shared, how it is shared, and with whom it is shared (Xiao-qing, Qing-xiang & Mang, 2010). Smart and sophisticated hackers with a great deal of technical competency and expertise spread malicious codes, such as viruses and Trojan horses in the virtual communities. These risks arise from the characteristics of knowledge in security. Knowledge of information security can be a piece of programing code, hyper link or file of software. By virtue of the risk, Gordon (1995) advised not to take candy from strangers – that is, do not take files from people you do not know. Do not compile a program or run a script, click on a link that you do not understand. Baird, Jamieson and Cerpa (2003) classified individuals who share knowledge in a virtual community into three categories. The first groups are those individuals who are smart and informed enough to support others. The second groups are those people who are not smart and capable enough to support others. They may or may not be supportive. The third groups are those individuals who are not only misinformed but are also malicious. Such individuals with malicious activities cause damage when they encounter an easy target. These hackers wait for those people who need help. When such people request help from them, they will receive advice from hackers that is in fact a harmful threat.

The contradictory opinions about whether security knowledge sharing in a professional virtual community can decrease or increase risks has led us to empirical research

concerning the relationship between knowledge sharing behavior and risk reduction. Accordingly, the last hypothesis of study would be:

Hypothesis 5. Knowledge sharing behavior is positively related to information security risk reduction in PVCs.

3.5 Second Research Model

The research model adopted for this study is depicted in Fig. 3.2. This model is based upon the aforementioned discussion and concepts. It includes six determinants: information security knowledge sharing behavior, perceived consequences, affect, social factor, facilitating condition, and risk reduction. It explains the relationship between perceived consequences, affect, social factor, and facilitating conditions with knowledge sharing behavior in PVCs. Furthermore, it displays the effects of knowledge sharing behavior on information security risk reduction. The perceived consequences are formulized into a model to be a formative construct and all of the other constructs were modelled using reflective indicators. With regard to this model, five hypotheses have been examined. Each hypothesis is depicted by H, and a number. The plus symbol shows a positive relationship, whereas the arrows show the hypothesized relationship.

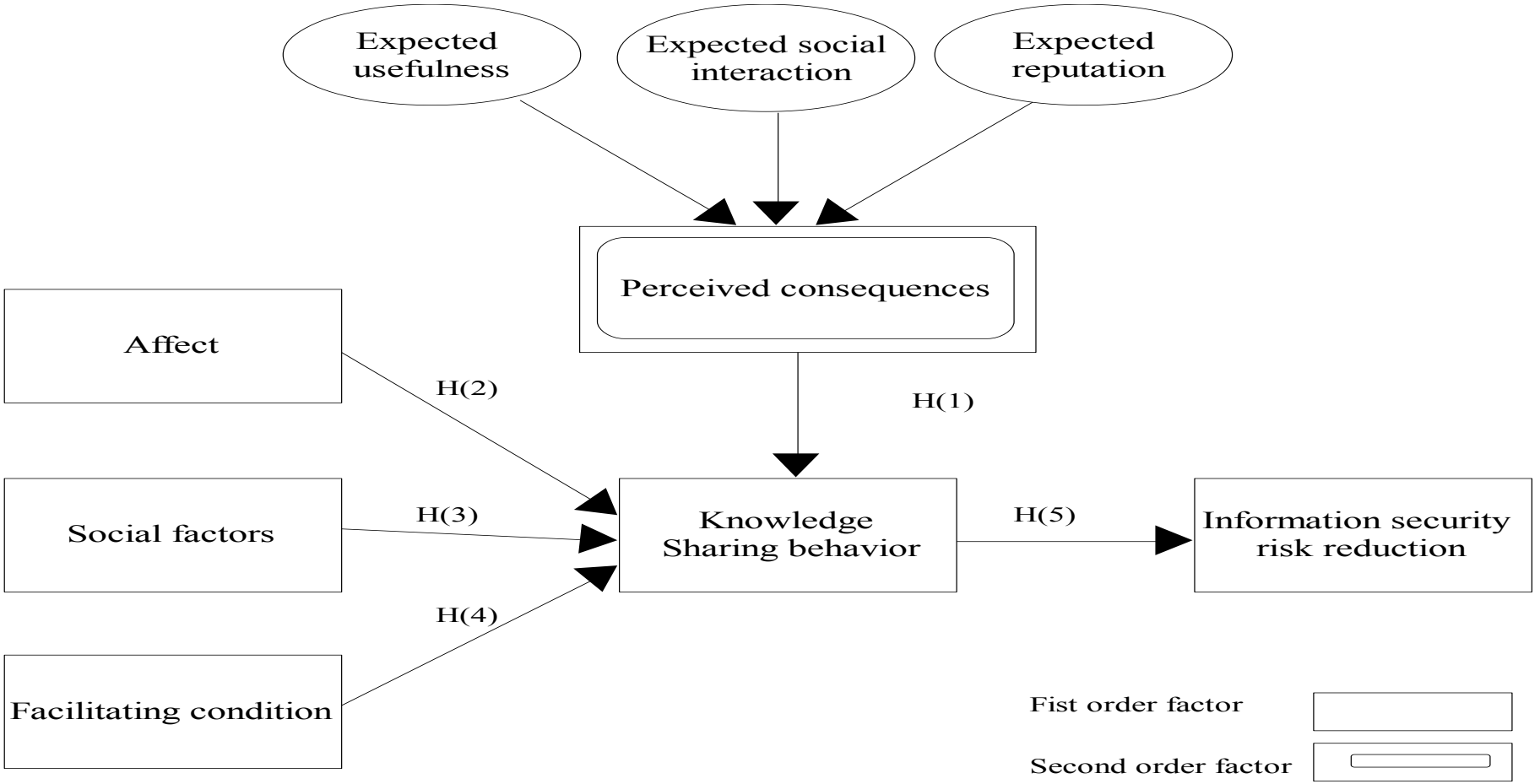

Figure 3.2 Second Research Mod

3.6 Summary of Chapter

This chapter develops two research models comprised of determinants derived from a review of the literature. The determinants of the first model includes attitude, self-efficacy, trust, norm of reciprocity, and shared language, in respect of the information security workers intention to share knowledge in PVCs. Based on these variables, 9 hypotheses and first research model are presented. Perceived consequences, affect, social factor, facilitating condition, knowledge sharing behavior and information security risk reduction are established as determinants of the second research model. According to these variables 5 hypotheses and second research model are presented. Next chapter describes the research design of this study to test the hypotheses developed in this chapter.

CHAPTER 4

RESEARCH METHODOLOGY

4.1 Introduction

This chapter describes the research design of the study to test the hypotheses developed in Chapter 3. The measures of each determinant are discussed in the next section. Comprehensive survey instruments were constructed to measure the determinants of the research models. A pre-test and pilot test was conducted to improve the survey instrument. The instruments of research models are included in this chapter. The reliability of the survey instruments are discussed as well. After assessing the reliability of the instruments, the data collection process is presented. In data collection section, the demographic characteristic of the survey respondent is reported. At the end of chapter, the selection of the data analytical technique and software is discussed.

4.2 Determinants Measures

In the present study, the items that are used to operationalize the constructs or determinants and are included in every examined model were mainly adapted from previous studies and modified for use in the information security knowledge sharing context.

In the first research model, some items and concepts taken from the studies of Hsu and Lin, Lin and Huang (2008), and Fang and Chiu (2010) were applied to investigate knowledge sharing intention. The concepts and items used to assess knowledge sharing attitude were adapted from Hsu and Lin (2008), and Chang and Chuang (2011). Self-efficacy was examined according to Fang and Chiu (2010), and Hsu, Ju, Yen and Chang (2007). Information and identification-based trust were examined according to Hsu, Ju,

Yen and Chang (2007), and content-based trust was assessed through concepts and items taken from Chang and Chuang (2011).

Information-based trust, identification-based trust, and content-based trust were utilized as indicators to build the superordinate trust determinant. The ideas and findings of Wasko and Faraj (2005) were applied to assess reciprocity. In these studies, the fairness of knowledge sharing has been the focal point. A shared language was measured with items adapted from Nahapiet and Ghoshal (1998). Tables 4.1 and 4.2 describe the definitions and questionnaire items of the first research model determinants, respectively.

Table 4.1 Definition of First Research Model Determinants

Constructs	Definition	Items
Intention	The extent to which information security workers believe they will adapt knowledge sharing actions.	4
Attitude	The degree to which information security workers has positive personal feelings to share knowledge.	6
Self-efficacy	The belief that one is capable of performing knowledge sharing.	4
Information-based trust	Members' trust toward virtual communities due to sound privacy and technology mechanisms.	3
Identification-based trust	Members' trust toward virtual communities due to emotional interaction among participants.	4
Content-based trust	Members' trust toward virtual communities due to quality and content of shared knowledge among participants.	3
Norm of reciprocity	Exchange of knowledge among information security virtual communities are mutual and perceived by the parties as fair.	4
Shared language	The acronyms, subtleties, and underlying assumptions that are the staples of interactions among information security workers.	3

Table 4.2 Questionnaire Items of First Research Model

Intention	1. If I find new vulnerability I will inform ISVC members. 2. If I find new threat I will inform ISVC members. 3. If I find a solution for a threat I will share with Information Security Virtual Community (ISVC) members. 4. I intend to share my security knowledge with Information Security Virtual Community (ISVC) members.
Attitude	1. Security knowledge sharing with ISVC members is an enjoyable experience. 2. Security knowledge sharing with ISVC members is valuable to me. 3. Sharing of security knowledge with ISVC members is always beneficial. 4. I am interested in participating in ISVC. 5. It is important for me to participate on ISVC. 6. Overall, my attitude towards ISVC is favorable.
Self-efficacy	1. I am sure that I can post new issues on ISVC discussion forum. 2. I am sure that I can give a response to a specific issue on ISVC discussion forum. 3. I am sure that I can discuss security-related issues on ISVC. 4. I am sure that I can chat on a specific topic on ISVC.
Information-based trust	1. ISVC has enough safeguards to make me feel comfortable to divulge personal information. 2. ISVC does not use personal information for any purpose unless it has been authorized by the stakeholder. 3. ISVC never sells members' personal information kept in its computer databases. 4. ISVC protects personal information from unauthorized access.
Identification-based trust	1. I can talk freely to the ISVC members about my personal issues. 2. Members on ISVC are truthful in dealing with one another. 3. I have faith in ISVC members.
Content - based trust	1. The knowledge shared by members on ISVC is accurate. 2. The knowledge shared by members on ISVC is complete. 3. The knowledge shared by members on ISVC is reliable.
Norm of reciprocity	1. I find that writing and commenting on ISVC can be mutually helpful. 2. When I share my knowledge through ISVC, I expect somebody to respond when I'm in need. 3. When I share my knowledge through ISVC, I believe that my queries for knowledge will be answered in future. 4. If I share my knowledge with other ISVC members, I will make more friends.
Shared language	1. Security terms and jargon are used on ISVC is understandable. 2. Shared acronyms and language facilitate understanding on ISVC. 3. On ISVC, we use common vocabulary to understand each other easily.

In the second research model, some items and concepts taken from the studies of Hsu et al. (2007), and Lin et al. (2009) were applied to investigate knowledge sharing behavior. Reputation-based consequence, social interaction-based consequence and usefulness-based consequence were utilized as indicators to build the superordinate perceived consequences construct. The usefulness-based perceived consequence was coined by Cheung et al. (2000), and Al-Khaldi and Olusegun (1999). The social interaction-based perceived consequence was assessed through variables taken from Huang (2009); Chang and Chuang (2011). The reputation-based perceived consequence was examined according to Chang and Chuang (2011), Hsu and Lin (2008). The ideas and findings of Jeon, Kim, and Koh (2011) were applied to assess affect. The social factor was operationalized according to Bergeron et al. (1995), and Hsu and Lin (2008). The facilitating condition was measured with items adapted from Jeon, Kim and Koh (2011). The risk reduction variable measurement was based on definitions and studies of Feledi, Fenz and Lechner (2013); Feledi and Fenz (2012), and Tamjidyamcholo et al. (2013). Table 4.3 illustrates the questionnaire items for the second research model determinants.

Table 4.3 Questionnaire Items of Second Research Model

Knowledge sharing behavior	1. I frequently share my expertise from my education or training with LinkedIn members 2. I frequently participate in knowledge sharing activities in LinkedIn. 3. I usually spend a lot of time conducting knowledge sharing activities in LinkedIn. 4. When participating in LinkedIn, I usually actively share my knowledge with others.
Usefulness	1. Knowledge sharing in LinkedIn would decrease the time needed for my job responsibilities. 2. Knowledge sharing in LinkedIn would increase the effectiveness of performing job task. 3. Considering all aspects, knowledge sharing in LinkedIn would be useful
Social interaction	1. I spend a lot of time interacting with some members in LinkedIn 2. I have frequent communication with some members in LinkedIn. 3. I maintain close social relationships with members in LinkedIn.
Reputation	1. Sharing my knowledge improves my reputation within LinkedIn community. 2. I feel that participation improves my status in LinkedIn.
Affect	1. My knowledge sharing in LinkedIn provides me with lots of happiness. 2. My knowledge sharing in LinkedIn gives me energy for my working life. 3. I feel good to support other participants to solve problems in LinkedIn.
Social factor	1. People who are important to me think that I should participate in LinkedIn. 2. People who influence my behavior encourage me to participate in LinkedIn. 3. My colleagues think that I should use LinkedIn.
Facilitating conditions	1. Specialized instruction, concerning knowledge sharing in LinkedIn, is available to me. 2. A specialized person (or group) is available for assistance with my knowledge sharing process in LinkedIn. 3. Guideline is available to me in the usage of LinkedIn.
Information security risk reduction	1. By sharing knowledge within LinkedIn, we can find better solution for our problem. 2. By sharing knowledge within LinkedIn, we can reduce probability of vulnerability. 3. By sharing knowledge within LinkedIn, we can reduce risk in information security

4.3 Survey Instrument Reliability

A group of items has been selected from the topics that were formerly discussed in order to quantify and measure research models determinants. A pre-test and a pilot-test were conducted prior to performing the final and formal survey in order to validate the research instrument.

In the first model, pre-test comprising a questionnaire, was devised by a group of five experts in the IS area, all of whom were undertaking PhD courses and using the same room as the researcher. They took into account the factors of ease of understanding, logical consistencies, contextual relevance, and sequence of items to assess the questionnaire. Their comments on the questionnaire were used to make a few minor corrections concerning item sequence and wording. For the pilot test, the questionnaire was emailed to the Computer Science Faculty through the email server of the university. Four professors, 8 PhD students and 20 master students who had been members of different professional virtual communities took the survey or questionnaire. All comments and suggestions about item structure and contents were collected.

In the second research model, two information system specialists along with two information security experts and two PhD students pre-tested the questionnaire. The PhD students are currently performing research on PVCs. Respondents were asked to comment on a list of items that corresponded to the constructs, including ease of understanding, logical consistencies, contextual relevance, and sequence of questionnaires. Furthermore, the pilot-test was conducted by twenty-seven members in Cloud Security Alliance (CSA), Cyber Security Forum Initiative (CSFI) and Information Systems Security Association (ISSA) discussion forums hosted by LinkedIn. Conducting the pre-test and pilot-test led to just a number of slight changes in the questionnaire, and it was not necessary to eliminate any statement. After adjusting

the minor changes and reviewing the questionnaire by two other expert academics, the instrument was ready to be sent in a large sample for the purpose regarding the data collection of the examination of our research model.

Multiple items were used to measure all the determinants, and all the items were measured using a five-point Likert-type scale (ranging from 1 = strongly disagree to 5 = strongly agree).

4.4 Data Collection

PVCs without rich knowledge are of limited value. Information security is often considered to be an intense cognitive activity that requires collaborative problem solving. PVCs have emerged due to new advancements and innovations in Internet technology. Such communities have been created as novel organizational supplementary tools to foster knowledge development, generation of value and social welfare. Professionals and experts can benefit from an environment created by VCs to share knowledge regarding career culture, problems identification, solution techniques, and professional virtue and behavior. Virtual communities can also play a major role in the educational sector. They can be used to expand the ecosystem and build a basic framework for cooperative learning. Novel social relationships, behavior models, and new methods of sharing and inventing knowledge can be created by VCs.

The population of the first model consisted of information security engineers and technicians in PVCs. This population included the Information Security Professional Association (ISPA), Information Systems Security Association (ISSA), Society of Information Risk Analysts (SIRA), and LinkedIn security groups. The target participants were security professionals on VCs.

The selected VCs provides educational forums, continuous learning framework, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

The Malaysia Society, Section 7 Act 1966, on the second of March 2011 is formally registered as Information Security Professional Association of Malaysia (ISPA.my). ISPA.my is made through the strong support and assistance from CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation of Malaysia (MOSTI). ISPA.my is actually the highest regarded association that is targeted on the development associated with Information Security Professionals in-line with the government's vision to create and sustain a safer cyberspace in order to enhance wealth creation, social well-being and National sustainability. ISPA.my is dedicated to offer continuous learning, professional educations as well as certifications and a common framework of professional conduct which permitting these types of professionals to channel, connect themselves to and raise themselves towards a better standard of professionalism within their work, society and public as a group of trustworthy Information Security specialists.

Information Systems Security Association (ISSA) is the community of choice for international cyber security professionals focused on managing technology risk, enhancing individual growth and securing critical information and infrastructure. The ISSA is an international, not-for-profit, organization of information security practitioners and professionals. It provides peer interaction opportunities, educational forums and publications that improve the skill, knowledge, and also professional development of its members. The main objective of the ISSA is to enhance management practices that makes sure the availability, integrity, and confidentiality of information

resources. The ISSA promotes education and interaction in order to generate a more successful environment for the professionals and for the global information systems security engaged. Practitioners include members at all levels of the security subject within a wide range of industrial sectors for example education, communications, manufacturing , financial ,healthcare, and government.

ISSA is focused on offering the subsequent services for the information security community: improve the education as well as broaden the skills and knowledge of its practitioners within the related fields of information systems security and information processing; promote a totally free changing of information security approaches, techniques, and also problem solving via its participants; offer communication to maintain practitioners up to date with present events in information processing and security as well as supplying advantages for them and to their employers; communicate with management, and with systems and information processing professionals the significance of implementing controls essentials to make sure the secure organization and utilization of information processing resources.

The Society of Information Risk Analysts (SIRA) is dedicated to continually improving the practice of information risk analysis. SIRA endeavour to do this by supporting the collaborative efforts of their members through research, knowledge sharing, and member-driven education.

Since the whole of SIRA will always be greater than the sum of its parts, SIRA value, above all else, the participation of their members. SIRA understand that it is their willingness to contribute openly and constructively that will help the society reach its mission of continual improvement. To that end, SIRA promotes the collaborative efforts if its members by offering a variety of connection methods, online and off, print and electronic, challenging traditional limitations with new technology and passion.

LinkedIn is a PVC in which individuals with professional occupations take part. This virtual community was founded in December 2002 and launched on May 5, 2003. Professional networking is the primary activity of this community. In June 2013, LinkedIn publicized a report stating that it had managed to attract more than 225 million appliers in more than 200 countries. In addition, it has upheld the creation of interest groups and on March 29, 2012, there were 1,248,019 such groups. The number of members in these groups ranges from 1 to 744,662. The biggest groups are mainly active in the employment sector; however, members of such communities discuss a wide range of topics relating to the professional and employment sectors. Presently, 128,000 such groups are active in academic and corporate alumni. LinkedIn covers nearly all dimensions of information security, and possesses more than 2,229 information security groups. A large number of commercial, government and academic organizations are typified by these groups. LinkedIn members have access to many beneficial services and tools for knowledge sharing. These services and tools are provided by LinkedIn information security groups, and include services, such as finding experts, electronic bulletin boards, technical forums, e-mail services and looking for or advertising jobs.

In the first research model, Google Form technology used to create online survey form. The link of the online questionnaires was emailed to members of PVCs from July 11 to September 18, 2012. The first page of the questionnaire explained the purpose of this study and ensured the confidentiality. By the time this survey was concluded, 157 questionnaires were collected. The exclusion of 19 invalid questionnaires resulted in a total of 138 complete and valid ones for data analysis. The respondents comprised chief information security officers (CISO) (7.2%), security managers (17.4%), security administrators and analysts (10.9%), security technicians (9.4%), security consultants

(30.4%), help desk personnel (7.2%), and others (17.4%). The descriptive characteristics of the respondents are depicted in Table 4.4.

Table 4.4 Characteristics of Respondents for First Model

Measure	Items	Frequency	Percent (%)	Measure	Items	Frequency	Percent (%)
Gender	Male	105	76.1	Education	High School	11	8
	Female	33	23.9		Bachelor	26	18.8
					Master	40	29
Age	18-25	11	8		Doctor	61	44.2
	26-30	26	18.8				
	31-40	40	29	Position	Chief Information Security Officer(CISO)	10	7.2
	Over 41	61	44.2		Security Manager	24	17.4
					Security Administrators and Analysts	15	10.9
Work - experience	0-5	44	31.9		Security Technician	13	9.4
	5-10	17	12.3		Security Consultants	42	30.4
	More than 10 years	77	55.8		Help Desk Personnel	10	7.2
					Others	24	17.4

In the second research model, the cover letter as well as the research participation information form was specifically designed for this study to inform the participants the purpose of the survey and the participants' rights as research subjects. The research participation form notifies the participants that the participation in the survey is completely voluntary and anonymous and provides the assurance that the data will be treated with strictest confidentiality.

Ten of the most active information security groups, as PVCs in LinkedIn, were selected for the analysis of the second research model containing Information Security Community, IT Security Expert, Information Security Risk Management (SARMA), Security Source Online, Cloud Computing Security Community, Security Industry

Group, Intelligence & Security, IT Security and Audit Professionals, Security Leaders Group, and Information Security Network. First, we applied for membership of the groups. After we managed to obtain the membership, the active users of the groups were identified and then a personal email was sent to about 2,000 users of the groups in order to manage and improve group participation. The email included a hyperlink to a questionnaire created by Google form technology, and a brief explanation about the purpose of the study. Moreover, it was mentioned in the email that if respondents returned the completed questionnaire, they would receive the research results. Our emails were sent from January 25, 2013 until June 22, 2013 and participation in this survey was voluntary. Overall, 165 responses were received. After eliminating 23, which were invalid, we had 142 valid responses left for further analysis. Table 4.5 shows the demographic and characteristic profiles of the participants. The majority of the respondents had relatively high experience, which can be considered as an advantage.

Table 4.5 Characteristics of Respondents for Second Model

Measure	Items	Frequency	Percent (%)	Measure	Items	Frequency	Percent (%)
Gender	Male	129	90.8	Education	High School	10	7.0
	Female	13	9.2		Bachelor	50	35.2
					Master	71	50.0
Age	18-25	5	3.5		Doctor	11	7.7
	26-30	18	12.7				
	31-40	46	32.4	Position	Chief Information Security Officer(CISO)	12	8.5
	Over 41	73	51.4		Security Manager	25	17.6
					Security Administrators and Analysts	17	12.0
Work - experience	0-5	21	14.8		Security Consultants	39	27.5
	5-10	19	13.4		Academician	33	23.2
	More than 10 years	102	71.8		Others	16	11.2

4.5 Data Analysis Software

The suggested models of the study were tested via Partial least squares (PLS). Partial least squares is a multivariate analytic technique that is mainly used for path analytic modelling with latent variables (Baron & Kenny, 1986). Contrary to standard linear regression, multivariate normality is not necessary in PLS when it performs assessment of parameters. In addition, PLS is an appropriate technique for assessing theories in their early formation stages; therefore, causal models can easily and properly be tested by PLS (Davenport & Pruzak, 2000), which is true about the present study case. The partial least squares method was selected to examine both the measurement and the structural models in this study. The PLS is a method for latent structural equation modelling. It proposes that all the measured variance is to be defined (Saadé & Bahli, 2005). The PLS can be utilized to test hypotheses. In other words, it indicates where correlations may or may not exist, and makes suggestions and recommendations for subsequent testing (Chin, 1998). PLS analyses, containing significance tests for path coefficients, were performed utilizing Smart PLS Version 2.0 (Ringle, Wende & Will, 2005). Two important points were considered in the selection of PLS (Chin, Marcolin & Newsted, 2003; Tiwana & Mclean, 2003): (1) PLS is able to formulate a reflective or formative model for latent constructs and (2) in terms of sample size, the PLS method demands considerably fewer requirements to verify a model than the alternative structural equation modelling techniques (e.g., LISREL, EQS, COSAN, and EZPATH). The present research models are analysed in the context of the measurement model and structural model. Initially, the measurement model was applied to verify if the determinants had adequate reliability and validity, and then the structural model was used to evaluate the relationships proposed in our research model. Data analysis was performed by PLS software (smart PLS 2.0). Furthermore, SPSS 19.0 was used to

analysis the Variance Inflation Factor (VIF). The VIF was used to assess the multicollinearity.

4.6 Summary of Research Design

In this chapter, a survey instrument was developed to test the hypotheses. A pre-test and pilot test was conducted to improve the survey instruments reliability. After refining the survey questions, a link to the Web-based survey was announced within the virtual communities. 138 valid responses were obtained and analyzed for the first research model. 142 valid responses were obtained and analyzed for the second research model. Demographic information regarding the sample is also presented. At the end of chapter, data analysis software is introduced.

CHAPTER 5

DATA ANALYSIS AND RESULTS

5.1 Introduction

A field study was conducted to test the proposed models and hypotheses, and the data collected were used to examine the measurement model and structural model. This chapter provides a thorough description of the analyses and results. It begins with a description of the data analysis methods including measurement model, structural model, and multicollinearity test, followed by presenting the result of the research models. The findings of each research model is presented separately.

First model analyses key factors, consist of attitude, self-efficacy, trust, norm of reciprocity, and shared language, with respect to the information security workers' intention to share knowledge. The second model is composed of two main parts. The first part is the Triandis theory, which is adapted to analyse the other determinants of knowledge sharing behavior in PVCs. The second part explores the quantitative relationship between knowledge sharing and security risk reduction.

5.2 Data Analysis Method

Smart PLS 2.0 was used to analysis collected data for the research models in the context of the measurement model and structural model. In addition, the Variance Inflation Factor (VIF) was used to assess the multicollinearity.

5.2.1 Measurement Model

At the measurement level, measurement items (indicators) used for each latent variable were estimated in terms of item loadings, internal consistency, and convergent and discriminant validities (AVE analysis).

5.2.1.1 Factor Analysis

Factor analysis was performed to extract the separate constructs for the main variables. Factor analysis examines the pattern of covariance between observed measures. Measures that are highly correlated (either positively or negatively) are likely influenced by the same constructs, while those that are relatively uncorrelated are likely influenced by different constructs.

In general, there are two types of factor analysis: exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). EFA is used to explore data to determine the number of, or the nature of, factors that explain the covariance between variables, while CFA examines whether a specified set of constructs is influencing responses in a predicted way. In brief, EFA is a theory-generating method. To verify the validity of these existing and proposed constructs, in this study, both CFA and EFA were employed.

Items belonging to the constructs were explored with factor analysis. Items were selected when factor loading is greater than 0.4(method: principle components) on the hypothesized factors. This criterion was considered appropriate in this study in order to create homogeneous and robust scales.

5.2.1.2 Reliability and Validity Analysis

In this section, reliability and validity of individual items are inspected. Reliability is the consistency of a set of measurements. Reliability is the degree to which a variable or concept is measured consistently. Validity refers to the degree to which measurements are actually measuring the variables they are purported to measure .

5.2.1.2.1 Individual Item Reliabilities

Individual item loadings and internal consistency were examined as a test of reliability. Individual item loadings that is greater than 0.7 are considered to be adequate (Chin & Newsted, 1999). This demonstrates that there is sound internal reliability. In addition, internal consistency was assessed through Cronbach's alpha. The desired lower limit for Cronbach's alpha is 0.6 (Hair, Anderson, Tatham, & Black, 1998).If Cronbach's alpha is bigger than 0.6, then, the internal consistency of the measurement scales is verified. In other words, the various questions for each construct measured the same construct.

5.2.1.2.2 Convergent and Discriminant Validities

Reliability tests look only at the items in the scale and do not compare across constructs. To compare one variable with other variables, a validity test should be performed. After the dropout and modification of measures from the previous confirmatory factor analysis, two additional validities were employed to ensure the validity of measures. Convergent validity and discriminant validity are both considered subcategories of construct validity.

Composite reliability and average variance extracted were calculated for assessing convergent validity. The minimum recommended level of reliability is 0.7 (Hair, Anderson, Tatham, & Black, 1998). Composite reliability was used to further assess the inter-item reliability. The minimum desirable level of average variance extracted (AVE) is 0.5 (Fornell & Larcker, 1981; Gefen, Straub, & Boudreau, 2000). Convergent validity adopts the measure of Average Variance Extracted (AVE) to gauge the percentage of explained variance by indicators relative to measurement errors. AVE value can also be used to measure the amount of variance that a latent variable component captures from its indicators. Fornell and Larcker (1981) suggest AVE should be greater than 0.5 to account for 50% or more variance of indicators.

The way to establish discriminant validity is to compare the square root of the AVE of each construct to the correlations of this construct to all other constructs. Fornell and Larcker (1981) suggested that the square root of AVE should be greater than the corresponding correlations among the latent variables. This result ensures that the measurement model has the discriminant validity (Chin, 1998).

5.2.2 Structural Model

The data analysis method employed in this study is the structural equation modeling (SEM) technique. SEM allows complicated relationships among variables to be expressed through structural equations and allow a more complete picture of the research model (Gefen et al., 2000).The structural model investigates the strength and direction of the relationships among theoretical latent factors. The structural model and hypotheses are tested by examining the path coefficients. In addition to the individual path tests, the explained variance (R-squares) in the dependent factors is assessed as an indication of the overall predictive strength of the model.

5.2.3 Multicollinearity

Another concern that needed to be addressed was multicollinearity. Collinearity is a condition that exists when two predicators (i.e., independent variables) correlated very strongly (Meyers et al. 2006), indicating that they may be two similar measures of the same thing (Tabachnick & Fidell 2006). Correspondingly, Multicollinearity is a condition that exits when more than two predicators are very highly correlated. As a general rule of thumb, it is recommended that two variables with a bivariate correlation in the middle 0.7s or higher should probably not be used in the same analysis (Allison

1999; Meyers et al. 2006; Tabachnick and Fidell 2006). The Variance Inflation Factor (VIF) was used to assess the multicollinearity. The VIF measures the degree of linear association between a particular independent variable and the remaining independent variables in the analysis. According to the rule of thumb, VIFs above 10 or tolerances below 0.1 are seen as a cause of concern, and need further investigation (Ho, 2006; Landau & Everitt, 2003). In this study SPSS 19.0 was used to analysis the VIF.

5.3 Result

In the following sections, the results of models are presented.

5.3.1 First Model Result

First proposed model is investigated in terms of measurement and structural models.

5.3.1.1 Measurement Model

Test of reliability was performed using individual item loadings and internal consistency. Individual item loadings that is greater than 0.7 are considered to be adequate (Chin & Newsted, 1999). As shown in Table 5.1, loadings for all measurement items are above 0.7. This demonstrates that there is sound internal reliability. In addition, internal consistency was assessed through Cronbach's alpha. As shown in Table 5.1, the Cronbach's alpha for all constructs is greater than 0.7.

Multiple approaches can be applied to estimate second-order factors (Chin, Marcolin & Newsted, 2003). The repeated indicator approach, also known as the hierarchical component model, is the mostly applied approach to assess second-order factors (Lohmöller, 1989). A second-order factor is directly measured by using the items of all its lower-order factors. The second most used approach is to formulize a model for the pathways between lower-order and higher-order factors (Edwards, 2001). It is possible to utilize this approach in calculating second-order factors in PLS through

implementing plenty of first-order factors. The latter approach has been applied to generate the second-order variable (trust) in the present study.

Convergent validity and discriminant validity were assessed to validate the measurement model. Composite reliability and average variance extracted were calculated for assessing convergent validity. According to the PLS analysis, the minimum recommended level of reliability is 0.7 (Hair, Anderson, Tatham, & Black, 1998), and the minimum desirable level of average variance extracted (AVE) is 0.5 (Fornell & Larcker, 1981; Gefen, Straub, & Boudreau, 2000). In our study, 0.883 to 0.942 was the range of composite reliabilities, and 0.67–0.843 was the range of average variance extracted, both exceeding the threshold values for acceptable convergent validity. Furthermore, the square root value of average variance extracted for each construct was compared with the correlations between constructs in order to assess discriminant validity. As shown in Table 5.2, the square root value of average variance extracted for each construct was bigger than any correlation values with other constructs, thereby confirming the discriminant validity of the study.

In addition to the discriminant validity assessment, we also checked for multicollinearity due to the relatively high correlations among some factors. The VIFs in this study ranged from 1.605 to 2.750, which were acceptable.

5.3.1.2 The Structural Model

After the validity of the measurement model was approved, the hypothesized relationships were tested using structural equation modelling (SEM). These relationships are depicted in Fig.5.1. Table 5.3 summarizes the hypothesis results. The results illustrate that attitude, trust, and norms of reciprocity have significant effects on an individual's intention to share knowledge ($\beta=0.391$, $p<0.01$; $\beta=0.272$, $p<0.01$; $\beta=0.210$, $p<0.05$), verifying hypotheses 1, 2b, 3a. However, self-efficacy and shared

language did not show any meaningful or direct effect on the intention of information security experts and professionals to share knowledge in VCs (β=0.087, $p>0.1$; β=0.015, $p>0.1$), which was thoroughly opposed to the initial expectations. Accordingly, hypotheses 2a and 5a were not supported. The results also show that self-efficacy (β=0.276, $p<0.05$), trust (β=0.243, $p<0.1$), norms of reciprocity (β=0.243, $p<0.01$) significantly and meaningfully affect attitude, which supports hypotheses 2b, 3b, 4b. However, shared language again did not show any significant or meaningful effect on attitude, and left hypothesis 5b unsupported. The explanatory power of the research model is shown in Fig 4.1. The R-square (R^2) is a statistical measure that provides the percentage of variance in a dataset. Furthermore, it demonstrates the quality of the PLS model (Chin, 1998; Saadé & Kira, 2009). The R^2 value of 0.610 indicates that attitude mediates the relationship between self-efficacy and intention. However, self-efficacy does not show a significant effect on intention (0.087). In general, the model illustrates that 53.8% of the variance exists in attitude towards knowledge sharing, and 61% of variance is related to intention to engage in knowledge sharing.

Table 5.1 Measurement Model Result for First Model

Measures	Items		Composite reliability	Average variance extracted	Loading	Standard Error	t-value
Intention	IN 1	Alpha=0.899	0.929	0.767	0.883	0.02	44.378
	IN 2	Mean=1.75			0.905	0.021	43.088
	IN 3	S.D.=0.898			0.883	0.028	30.897
	IN 4				0.831	0.037	22.164
Attitude	AT 1	Alpha=0.915	0.934	0.701	0.849	0.0278	30.523
	AT 2	Mean=1.813			0.808	0.051	15.803
	AT 3	S.D.=0.877			0.786	0.049	15.917
	AT 4				0.859	0.034	25.095
	AT 5				0.859	0.019	45.036
	AT 6				0.866	0.039	21.934
Self-efficacy	SE 1	Alpha=0.901	0.931	0.772	0.834	0.033	25.194
	SE 2	Mean=1.926			0.857	0.033	25.835
	SE 3	S.D.=0.924			0.901	0.02	45.834
	SE 4				0.921	0.016	59.133
Information-based trust	INT 1	Alpha=0.9	0.93	0.769	0.833	0.036	23.14
	INT 2	Mean=2.225			0.888	0.026	33.539
	INT 3	S.D.=1.159			0.892	0.023	39.121
	INT 4				0.895	0.019	45.909
Identification-based trust	IDT 1	Alpha=0.838	0.902	0.755	0.876	0.019	46.471
	IDT 2	Mean=2.251			0.864	0.033	26.557
	IDT 3	S.D.=1.123			0.867	0.032	26.782

Continued Table 5.1

Content-based trust	COT 1	Alpha=0.907	0.942	0.843	0.902	0.027	33.734
	COT 2	Mean=2.21			0.913	0.018	50.524
	COT 3	S.D.=1.067			0.939	0.011	87.147
Norm of reciprocity	NR 1	Alpha=0.837	0.89	0.67	0.85	0.024	34.771
	NR 2	Mean=1.735			0.851	0.031	27.426
	NR 3	S.D.=0.839			0.768	0.08	9.604
	NR 4				0.803	0.068	13.008
Shared language	SL 1	Alpha=0.802	0.883	0.716	0.834	0.033	25.564
	SL 2	Mean=1.918			0.859	0.029	29.081
	SL 3	S.D.=0.955			0.846	0.04	21.335

Table 5.2 Correlation between Research Determinants for First Model

	IN	AT	SE	INT	IDT	COT	NR	SL
IN	**0.876**							
AT	0.609	**0.838**						
SE	0.565	0.625	**0.879**					
INT	0.642	0.599	0.555	**0.869**				
IDT	0.631	0.552	0.544	0.752	**0.877**			
COT	0.633	0.694	0.689	0.738	0.7	**0.918**		
NR	0.669	0.66	0.614	0.626	0.673	0.699	**0.819**	
SL	0.346	0.442	0.574	0.492	0.463	0.546	0.461	**0.846**

Note: IN, intention; AT, attitude; SE, self-efficacy; INT, information-based trust ;IDT, Identification-based trust; COT, content-based trust; NR, norm of reciprocity; SL, shared language.
The bold numbers in the diagonal row are square roots of the average variance extracted.

Table 5.3 Results of Hypothesis Testing for First Model

Hypotheses	Results
H1. Attitude to sharing knowledge affect positively on individuals knowledge sharing intentions.	Supported
H2a. Individuals' self-efficacy is positively associated with their intentions toward knowledge sharing.	Not supported
H2b. Individuals' self-efficacy is positively associated with their attitudes toward knowledge sharing.	Supported
H3a. Trust is positively associated with the individuals' intentions of knowledge sharing.	Supported
H3b. Trust is positively associated with the individuals' attitudes of knowledge sharing.	Supported
H4a. Norm of reciprocity is positively associated with the individuals' intention of knowledge sharing	Supported
H4b. Norm of reciprocity is positively associated with the individuals' attitudes of knowledge sharing.	Supported
H5a. Shared language is positively associated with the individuals' intentions of knowledge sharing.	Not supported
H5b. shared language is positively associated with the individuals' attitudes of knowledge sharing	Not supported

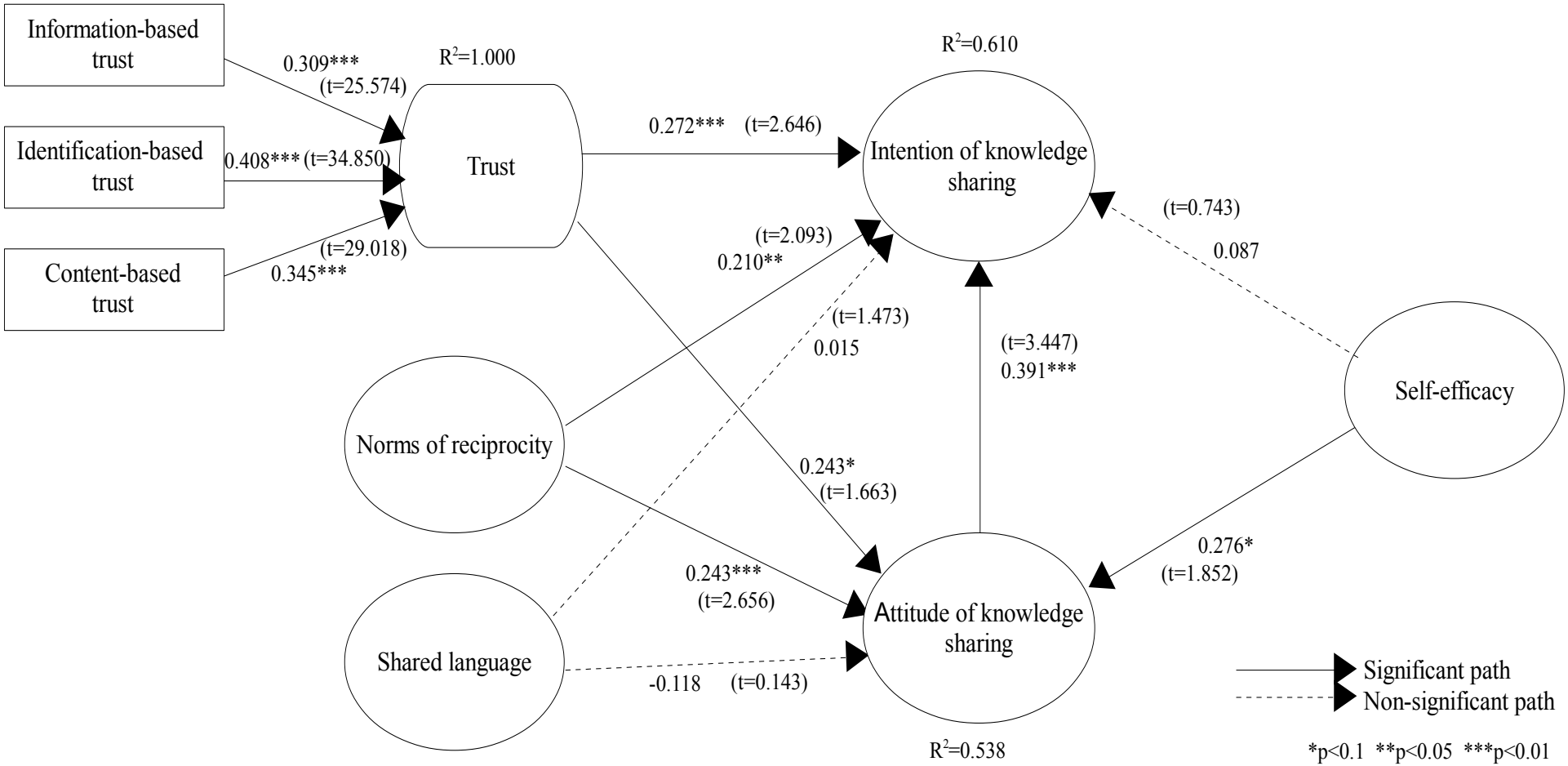

Figure 5.1 Results of SEM Analysis for First Model

5.3.2 Second Model Result

Second proposed model is investigated in terms of measurement and structural models.

5.3.2.1 The Measurement Model

Individual item loadings and internal consistency were examined as a test of reliability. Individual item loadings that are greater than 0.7 are considered to be adequate (Chin & Newsted, 1999). As shown in Table 5.4, loadings for all measurement items are above 0.7. This demonstrates that there is sound internal reliability. In addition, internal consistency was assessed through Cronbach's alpha. As shown in Table 5.4, the Cronbach's alpha for all constructs is greater than 0.7. Since this model incorporates one second-order variable (perceived consequences), we created a superordinate second-order construct using the factor scores of the first-order constructs (Chin, Marcolin & Newsted, 2003). We considered indicators of perceived consequences as formative because a drop in one indicator did not imply any change in the others (Hair, Anderson, Tatham, & Black, 1998).

Composite reliability and average variance extracted were measured for estimating convergent validity. According to PLS analysis, the lowest recommended level of reliability is 0.7 (Hair et al., 1998), and the lowest desirable level of average variance extracted (AVE) is 0.5 (Fornell & Larcker, 1981). In our study, 0.828 to 0.918 was the range of composite reliabilities, and 0.617–0.788 was the range of average variance extracted, both exceeding the threshold values for acceptable convergent validity. Discriminant validity is also measured via AVE. The square root of AVE should be greater than the correlations among the constructs. In other words, the extent of variance that exists in both a latent variable and its body of indicators must exceed the shared variance between the latent variables. The inter-correlations of constructs and variance that exist in both latent variables and their indicators are depicted in Table 5.5.

The square root of the AVE is represented by the diagonal elements in Table 5.5. This indicates that the square roots of every AVE value are bigger than the off-diagonal elements. It can be inferred that there is an acceptable and logical extent of discriminant validity in the assessment model with regard to all the determinants. In addition, measurement analysis outcomes demonstrate that the degree of discriminant validity in all determinants and measures is reasonable and adequate. Table 5.5 shows that the correlation in some variables is fairly strong and high; therefore, we perform the multicollinearity test. Since each variance inflation factor (VIF) value ranged from 1.368 to 2.421, multicollinearity did not seem to pose a threat.

5.3.2.2 The Structural Model

Since we have reached convincing results from the reliability and validity testing in the previous sections, we move on to testing our proposed hypotheses. In this section, we are going to assess our proposed model through structural equation modelling (SEM) to examine our hypotheses. The test of the structural equation model includes an estimation of the path coefficients and R2 values. The path coefficients indicate the strengths of the relationships between the endogenous and independent variables, and the R2 values represent the amount of variance explained by the independent variables. The results of hypothesis testing using PLS are summarized in Table 5.6. In Fig. 5.2, the R2 values, which reflect the predictive power of the model, are depicted within the oval of each endogenous variable. The model explains 99.3% of the variance in perceived consequences, 49.9% in knowledge sharing behavior and 18.1% of the variance in information security risk reduction. Fig. 5.2 also shows the results of the path coefficients. To realize the efficacy of the knowledge sharing factors in information security PVSs, we studied the path relationship between perceived consequences, affect, social factors, facilitating conditions and behavior. The path coefficient from perceived

consequences to behavior is positive, and it is statistically significant ($\beta=0.178$, $p<0.05$). This implies that perceived consequences were effectively influenced by knowledge sharing behavior; thus verifying hypothesis 1. The results show that affect ($\beta=0.471$, $p<0.01$), facilitating conditions ($\beta=0.127$, $p<0.05$) significantly and meaningfully affect knowledge sharing behavior, which confirms hypotheses 2 and 4. Contrary to our conjecture, the social factor had an insignificant effect on knowledge sharing behavior ($\beta=0.039$, $p>0.1$). Therefore, hypothesis 3 was not supported. Concurring with our initial assumption, the path coefficients indicate the strengths of the relationships between the knowledge sharing behavior and information security risk reduction ($\beta=0.426$, $p<0.01$). Therefore, hypothesis 5 was validated.

Table 5.4 Measurement Model Result for Second Model

Measures	Items		Composite reliability	Average variance extracted	Loading	Standard Error	t-value
Knowledge sharing behavior	KSB 1	Alpha=0.857	0.914	0.78	0.896	0.011	83.501
	KSB 2	Mean=2.694			0.928	0.007	126.48
	KSB 3	S.D.=1.068			0.821	0.023	35.909
Usefulness	US 1	Alpha=0.724	0.845	0.645	0.837	0.043	19.536
	US 2	Mean=2.427			0.809	0.027	30.339
	US 3	S.D.=0.842			0.763	0.071	10.836
Social interaction	SI 1	Alpha=0.729	0.828	0.617	0.831	0.021	39.078
	SI 2	Mean=2.38			0.828	0.031	26.745
	SI 3	S.D.=0.885			0.739	0.042	16.289
Reputation	RE 1	Alpha=0.865	0.918	0.788	0.844	0.028	29.809
	RE 2	Mean=2.288			0.901	0.023	39.245
		S.D.=0.835					
Affect	AF 1	Alpha=0.822	0.894	0.737	0.829	0.017	49.34
	AF 2	Mean=2.549			0.878	0.025	35.03
	AF 3	S.D.=0.8			0.868	0.021	42.166
Social factor	SF 1	Alpha=0.838	0.899	0.749	0.911	0.019	48.942
	SF 2	Mean=2.708			0.916	0.014	67.172
	SF 3	S.D.=0.914			0.76	0.031	24.395
Facilitating conditions	FC 1	Alpha=0.714	0.841	0.641	0.878	0.023	38.861
	FC 2	Mean=2.542			0.847	0.056	15.008
	FC 3	S.D.=0.924			0.721	0.087	7.605
Information security risk reduction	RR 1	Alpha=0.78	0.86	0.673	0.892	0.025	35.49
	RR 2	Mean=2.488			0.826	0.031	26.269
	RR 3	S.D. =0.842			0.735	0.057	12.949

Table 5.5 Correlation between Research Determinants for Second Model

	KSB	US	SI	RE	AF	SF	FC	RR
Knowledge sharing behavior(KSB)	**0.883**							
Usefulness(US)	0.504	**0.803**						
Social interaction(SI)	0.458	0.588	**0.786**					
Reputation(RE)	0.563	0.628	0.711	**0.888**				
Affect(AF)	0.682	0.655	0.59	0.626	**0.858**			
Social factor(SF)	0.447	0.461	0.461	0.534	0.538	**0.865**		
Facilitating conditions(FC)	0.441	0.402	0.262	0.296	0.491	0.422	**0.801**	
Risk reduction(RR)	0.426	0.489	0.319	0.396	0.473	0.411	0.296	**0.82**

Note: The bold numbers in the diagonal row are square roots of the average variance extracted.

Table 5.6 Results of Hypothesis Testing for Second Model

Hypotheses	Results
Hypothesis 1. The perceived consequence is positively related to the knowledge sharing behavior of members in PVCs.	Supported
Hypothesis 2. The affect is positively related to the knowledge sharing behavior of members in PVCs.	Supported
Hypothesis 3. The social factor is positively related to the knowledge sharing behavior of members in PVCs.	Not supported
Hypothesis 4. The facilitating condition is positively related to the knowledge sharing behavior of members in PVCs.	Supported
Hypothesis 5. Knowledge sharing behavior is positively related to information security risk reduction in PVCs.	Supported

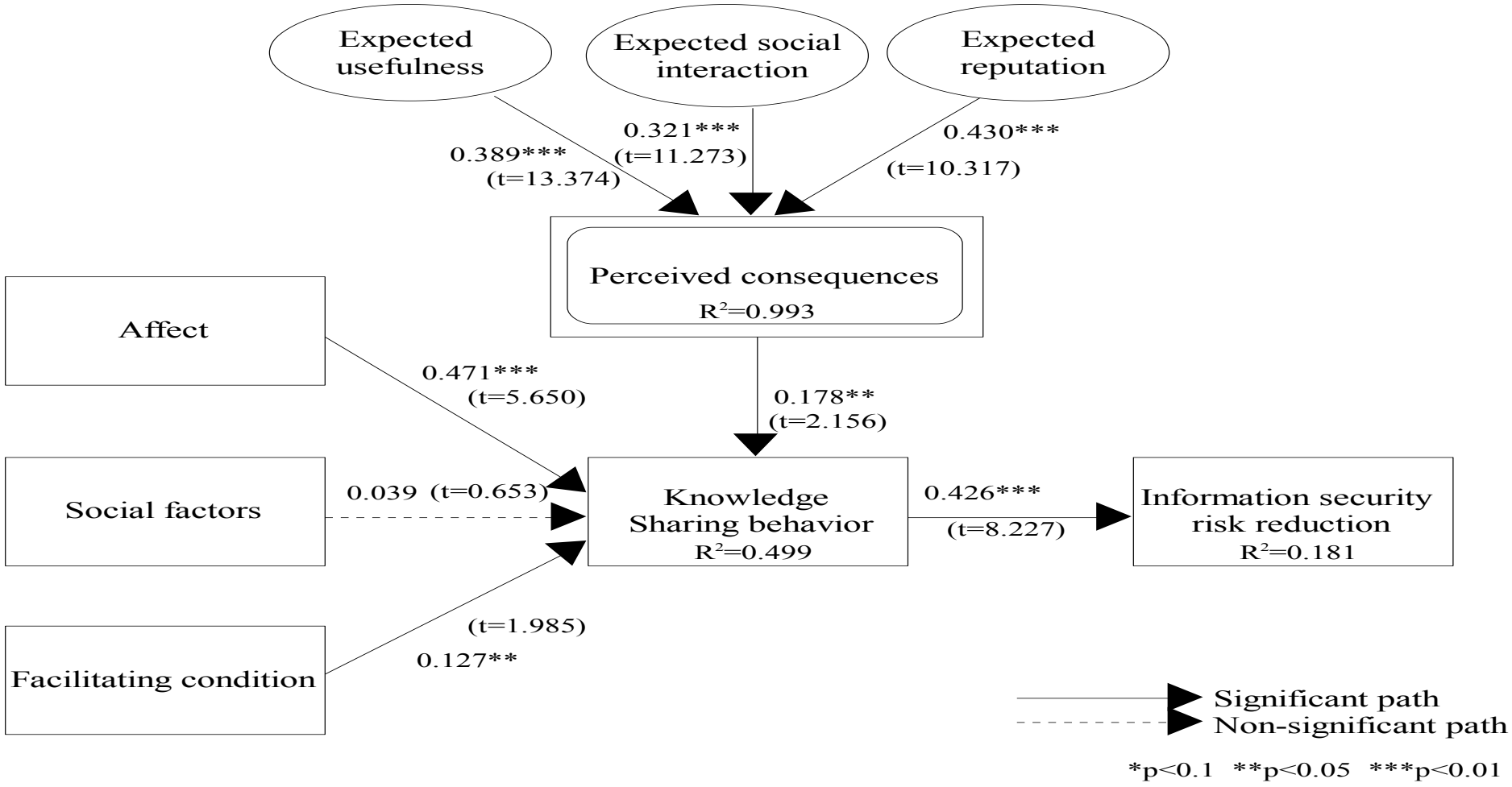

Figure 5.2 Results of SEM Analysis for Second Model

5.4 Summary of Chapter

This chapter presented the results of the study. Before examining the research hypotheses, factor analysis was conducted. Then, reliability and validity tests were conducted. The Cronbach's alpha verified the reliability of measures, and convergent and discriminant validity tests verified that the research variables were adequately measuring what were intended. Fourteen research hypotheses were empirically investigated utilizing path analysis. Six out of nine hypotheses of first model were supported. The results suggest a strong relationship between attitude, trust, and norms of reciprocity to knowledge sharing intention. Hypotheses regarding the influence of self-efficacy and reciprocity, to knowledge sharing attitude were upheld. Shared language did not influence either the attitude or intention to share knowledge. In the second model four out of five hypotheses were upheld. The results shows that perceived consequences, affect, and facilitating conditions have significant effects on knowledge sharing behavior. In contrast, social factors have shown insignificant effects on knowledge sharing behavior. The study demonstrates that there is a positive and strong relationship between knowledge sharing behavior and information security risk reduction.

CHAPTER 6

DISCUSSION AND CONCLUSION

6.1 Introduction

In the following chapter the result of the research models based on data analysis result of chapter 4 are discussed. Then, the findings of the research models in terms of practical and theoretical implications are explained. Afterwards, the conclusions of the research are presented. Lastly, the limitations of this study and recommendations for future research are discussed.

6.2 Discussion

In this section, findings and results of both models are discussed.

6.2.1 First Model

In the first model, as was discussed in the data analysis section earlier, the results show that attitude, trust, and norms of reciprocity significantly affect the intentional behaviour of knowledge sharing. Attitude, as suggested by previous research, shows the highest positive effect on an individual's intention to engage in knowledge sharing. Basically, attitude is believed to have a crucial role in people's intention (Bock et al., 2005). Those people who think highly of knowledge sharing and show a positive attitude and thoughts about it are more motivated to engage in knowledge sharing activities (Bock et al., 2005; Heinze & Hu, 2009).

As it has been verified by the results of the previous studies (Hasan, 2006; He & Freeman, 2010), the results of the present research show that self-efficacy has a positive effect on knowledge sharing attitude. Self-efficacy is acknowledged to be a vital construct in recognizing the information security activities of individuals (Agarwal, Sambamurthy & Stair, 2000; Compeau & Higgins, 1995; Thatcher & Perrewe, 2002).

Nonetheless, self-efficacy shows no direct or significant effect on knowledge sharing intention, which is totally against the initial expectations. It seems that self-efficacy may have an indirect effect on knowledge sharing, especially when it is accompanied by trust and norms of reciprocity.

Previous research (Chang & Chuang, 2011; Chow & Chan, 2008; Hsu et al., 2007; Hsu & Lin, 2008) has demonstrated that trust affects knowledge sharing directly and significantly. Likewise, the results of the present study show that trust, directly or indirectly, can affect both the intention and attitude of knowledge sharing in a positive manner. The participants of a community who have trust in each other are more enthusiastic and eager to communicate with each other. They like to know more about the skills and abilities of others. Our findings regarding Information-based trust and Identification-based trust are consistent with other studies (Hsu et al., 2007). In fact, when the members of a community get to know each other more seriously and profoundly, they will be able to gain a particular knowledge and capture it from others. In doing so, they will engage in knowledge sharing more easily. Quality and content of knowledge similar to Chang and Chuang's study (2011) has positive influence on forming comprehensive trust between contributors. In information security the shared knowledge could be a programming code or hyper link which receivers of the knowledge through running the code on his or her computer or clicking on the hyper link could be victim of the knowledge sharing process. Thus, trust on the shared content plays a significant role in information security field. Coleman (1988) contends that people only seek trust when they are in dangerous situations. Information security is believed to be a hazardous situation because the knowledge sharing of participants may cause harm and damage to the computers and systems of others. Hence, trust seems to be an influential and significant factor involved in knowledge sharing in the information security sector. The results of the current study confirm that participants of a VC like to

share their experience and knowledge with others to seek mutual gain. The results are similar to Wasko and Faraj's findings (2005). Accordingly, it can be suggested that the norms of reciprocity can significantly affect the intentions and attitudes of VC participants. Contrary to our assumptions, a shared language appears to have no significant effect on knowledge sharing intention and attitude. One possible explanation may be that the field study in this research is professional virtual communities (ISPA, ISSA, SIRA, and LinkedIn) and the participants of the communities know and understand one another language, shared jargon and vocabulary, therefore, the users of the communities may not consider shared language as a motivation to their knowledge sharing activities (Lin et al., 2008). An avenue for future research is to examine why a shared language doesn't influence on the intention and attitude of professional virtual communities' member to share their knowledge and information.

6.2.2 Second Model

The main objective of the second research model was to identify and understand the determinants of knowledge sharing behavior in PVCs and to investigate the quantitative relationship between knowledge sharing behavior and information security risk reduction. An empirical study was conducted to test the theoretical model. The results indicate that perceived consequences are the most significant determining factor for knowledge sharing behavior. The results of data analysis affirm that perceived consequences can play a major role in knowledge sharing activities in PVCs; therefore, it can be inferred that as the degree of perceived consequences increases, knowledge sharing activities will also increase. Three kinds of consequences have been identified by our proposed research model –expected usefulness, expected social interaction, and expected reputation. It has been shown by previous studies (Wasko & Faraj, 2000, Bock et al., 2005) that expected usefulness can directly and significantly influence knowledge

sharing. Accordingly, the finding of previous studies that there is a positive relationship between knowledge sharing and expected usefulness is supported by the results of the present study. Furthermore, the results of the present study confirm another important finding from the previous studies (Nahapiet & Ghoshal, 1998; Chang & Chuang, 2011); demonstrating that expected social interaction can positively affect knowledge sharing behavior. The knowledge of a professional virtual community consists of explicit and tacit components. It is possible for everyone to easily gain access to explicit knowledge through the Internet. However, tacit knowledge exists in the minds of community members and cannot be shared with others via social interaction. The results of other related studies show that social interaction bonds between members of a network can be reinforced by social interaction, and that it can be considered as a significant forecaster of collective action (Wasko & Faraj, 2005). These bonds will be built among people with similar and identical interests and resources rather than dissimilar people (Johnson, 2007). Thus, these bonds and connections assist in knowledge sharing and keeping members together. As confirmed by the results of other studies (Kankanhalli, Tan & Wei, 2005; Wasko & Faraj, 2005), expected reputation is shown to have a significant effect on knowledge sharing activities; therefore, PVCs can be described as an environment in which members are able to achieve reputation in their professional sector. This indicates that perceived consequences can still be regarded as the principal determining factor of knowledge sharing behavior, and it truly supports the findings of other related studies (Triandis, 1980; Jeon, Kim & Koh 2011). Another hypothesis of the model is also supported by the findings. This hypothesis states that knowledge sharing within PVCs is stronger when PVC members have positive feelings toward it; this hypothesis is also supported by the findings. This is in agreement with the results of Triandis (1980), and Bergeron et al. (1995). Intrinsic motivations of knowledge sharing are embodied in affect. Affect could influence community members in different

dimensions, including joy, enthusiasm, energy and happiness, which show that intrinsic motivations of knowledge workers can significantly affect knowledge sharing activities. The social factor was not found to be an influential element in information security virtual communities. This is consistent with the findings of the previous studies (Hsu & Lin 2008; Davis et al., 1989), which argued that social factors had no significant influence on blog and computer technology utilization behavior, but it is contradictory to the results of the earlier studies of Al-Khaldi and Olusegun Wallace (1999), and Bock et al. (2005), in which the social factor was shown to have an affirmative impact on PC usage behavior and the individual's intention toward knowledge sharing. One plausible explanation for this finding might be that more than seventy percent of participants of this survey have more than ten years' experience. Therefore, they are quite familiar with their benefits and know how and where to find the knowledge they need. That might be the reason why social factors have no effect on their behavior. The second possible explanation may be due to the fact that participants do not trust the ideas and influential acts of others while it is believed by many experts that trust is a significant component in information security knowledge sharing (Tamjidyamcholo et al., 2013). The third reason may be that acting in PVCs is voluntary and there is no obligation to participate in the knowledge sharing process. Venkatesh and Davis (2000) showed that the social factor has a significant effect while the environment is mandatory. Furthermore, as was discussed in the data analysis section earlier, the results show that facilitating conditions affect the behavior of knowledge sharing significantly, which is consistent with the findings of Jeon et al. (2011), and He and Wei (2009). Lastly, the relationship between knowledge sharing and factors like performance (Huang, 2009; Du, Ai & Ren, 2007), information systems outsourcing success (Lee, 2001), the effectiveness of IS/IT strategic planning (Pai, 2006), and firm innovation (Lin, 2007) was found to be positive. In this study, the relationship between knowledge

sharing and information security risk reduction was investigated. The results show that knowledge sharing behavior is a good way to effectively and efficiently reduce risk in information security. The results of this empirical research support Tamjidyamcholo et al. (2013), and Feledi, Fenz and Lechner (2013) who argued that knowledge sharing can reduce risk. The authors believed that if the security of information and knowledge can be shared between trusted participants, it will most likely decrease risk.

6.3 Implications

Theoretical implications and practical implications of the models are presented in this section.

6.3.1 Theoretical Implications

6.3.1.1 First Model

The findings of the first research model provide several important theoretical implications. First, this study provides an initial step towards understanding the effect of key factors, including attitude, self-efficacy, trust, norm of reciprocity, and shared language, in respect of the information security workers intention to share knowledge. Our results confirm that attitude, self-efficacy, trust, norm of reciprocity in information security is a meaningful construct in explaining users' security knowledge sharing intention. Second, this research also contributes to the field of information security new sub-dimensions for the trust construct – information-based trust, identification-based trust and content-based trust – to be applied in the virtual community knowledge sharing jargon. Our findings reveal that information-based trust, identification-based trust and content-based trust has to be established first, and then develop comprehensive trust. Only by forming these kinds of trusts, mutual trust will be formed. Trust is not a single or one-dimensional concept and develops gradually as the parties move from one stage to another (Boon & Holmes, 1991; Lander et al., 2004; Panteli & Sockalingam, 2005).

6.3.1.2 Second Model

From a theoretical point of view, the second research model presented here makes a number of important theoretical contributions. Firstly, we incorporate the elements from the well-established model of Triandis to investigate the knowledge sharing behavior in information security professional virtual communities. In light of the preceding arguments, perceived consequence, affect and facilitating conditions were found to be a meaningful construct in explaining the knowledge sharing behavior of information security experts. Secondly, this study rests on the literature, which has developed new sub-dimensions for the perceived consequences determinant, including expected usefulness, expected social interaction and expected reputation to fit the PVCs knowledge sharing context. The results imply that information security professionals affirm the entire body of consequences (usefulness, social interaction and reputation) in their knowledge sharing activity. Thirdly, we have analytically examined the effect of knowledge sharing behavior on information security risk reduction. Our findings indicate that knowledge sharing can decrease the risk of security. The assumption that knowledge sharing can increase risk would be a barrier to the knowledge sharing process. Thus, when this assumption is rejected, it will be possible to have a good motivation for the knowledge sharing process.

6.3.2 Practical Implications

6.3.2.1 First Model

Information security virtual communities are a channel that learners, technicians, and professionals through participating can advance their knowledge, solve problems, and share findings. From a practical perspective, the findings indicate that practitioner's viewpoints on their efficacy and ability in the information security domain has affirmative effect on their knowledge sharing attitude. Therefore, the virtual community

providers and managers need to design online training programmes and other supportive mechanism that more effectively foster the participants' efficacy. Moreover, the results suggest that the role of trust in all of the three features comprising information-based trust, identification-based trust, and content based trust is significant and has promising impact on both intention and attitude of knowledge sharers. Thus, it may be necessary for managers of professional VCs to make an affable environment (e.g., via holding periodic face-to-face meeting and enhancing online interaction and communication among members) where two parties involved in an interaction know each other well and understand each other's desires and emotions to raise individuals' information and identification-based trust. The VCs should provide a procedure to rank the contributors of the community based of their certification, experience, and other characteristics to show the shared content and knowledge validity. The high and low ranking of contributors shows scale of their knowledge validity. Finally, in the present research, norm of reciprocity significantly affect the intentions and attitudes of VCs participants. Hence, mangers should use extrinsic motivators such as reward systems for encouraging norms of reciprocity among practitioners of virtual communities. For example, the contributors of the knowledge receive value added points as an exchange of favours which prove their performance and attempt.

6.3.2.2 Second Model

In terms of the practical implications of the study, the providers of information security virtual communities need to pay attention to diverse motivational dimensions and establish an appropriate support system to strengthen each motivational dimension, to activate the knowledge sharing activities of PVCs members. Therefore, managers of the community should provide extrinsic and intrinsic motivations to enhance the participation of the members. This study proposes the following suggestions to help

practitioners manage or design better PVCs in order to foster knowledge sharing behavior among members. First of all, the results indicate that the expected usefulness, as a sub-dimension of perceived consequences, has a significant effect on knowledge sharing behavior. From the practitioners' standpoint, PVC managers should create an environment that participants would find the community useful. In doing so, they should improve the quality of community knowledge, which might be useful for participants via maintaining and attracting experienced individuals (e.g., providing reward system or introducing job opportunities). The findings of this study imply that expected social interaction significantly impacts the knowledge sharing behavior of members. Therefore, the administrators of the communities need to hold face-to-face meetings or seminars and invite top knowledge contributors and professional instructors to share their knowledge and experience with members of the community. This will enhance the social interaction ties among its members. They can also create personal message boards and blogs as tools for enhancing online communication and interaction among members. The results of this study indicate that expected reputation is an important component of perceived consequences. Thus, PVC developers should incorporate a built-in reputation feedback to the community because reputation feedback is believed to have a strong influence on knowledge sharing behavior. The quantity of members' contributions can be implemented as a system feature and would accordingly show the activity of the contributor. The implementation of a ranking mechanism for quality of contribution needs to be created, which allows for the quality ranking of members' ideas. In addition, the results show that affect has a positive effect on virtual knowledge sharing behavior. Thus, community managers should touch PVC members' emotions via establishing a community spirit. This can be achieved by diverse membership activities (i.e., online quiz, travel vouchers, online competition, etc.). Furthermore, facilitating conditions show a positive effect on the proposed model.

As was discussed earlier, PVC members would have extrinsic and intrinsic motivation for knowledge sharing within PVCs. However, knowledge sharing actions and activities would not be spread and promoted if the necessary supporting systems are not available. Hence, it is necessary for community managers to supply resources, such as supporting group, and specific instructions and guidance to foster the contribution of members. Lastly, the results of the present study reject the major assumption that knowledge sharing could pose a risk and threat that can impede the knowledge sharing process in security communities. Thus, community managers can apply this important finding to foster and promote the participation of members in the activities of information security professional virtual communities.

6.4 Conclusion

Overall conclusion of the first and second model is presented in this section.

6.4.1 Fist Model

The objective of this study was to investigate the determinant that affect on the intention of information security experts and professionals to share knowledge in VCs. Information security professionals in VCs were assessed to test the proposed research model. The results of the measurement model test, including convergent validity, discriminant validity, variance inflation factor, and explanatory power, were satisfactory. In accordance with the concepts and notions of literature, some factors, such as intention, attitude, self-efficacy, trust, norms of reciprocity, and shared language, were studied. These factors are believed to encourage and promote knowledge sharing in information security virtual communities. Trust and norms of reciprocity of security professionals were shown to positively affect their intention and attitude to share knowledge. Although self-efficacy was found to have a positive effect on attitude, it showed no significant effect on the intention of security professionals to

share knowledge. Shared language showed no significant effect on either the intention or attitude of technicians.

6.4.2 Second Model

We believe that knowledge sharing has become an important part of the virtual communities. Understanding the phenomena is essential for Internet-based communities. The main objective of this study was to investigate the factors that can affect the knowledge sharing behavior of information security professionals in professional virtual communities. Therefore, we developed a concise model of knowledge sharing behavior that took into account many important factors from the Triandis model. These factors are believed to encourage and promote knowledge sharing in information security virtual communities. In addition, the relationship between security knowledge sharing and risk reduction has been investigated in our proposed model. An empirical study was conducted to test the theoretical model. The theoretical model was assessed through the measurement model including the reliability, discriminant validity and variance inflation factor and the structural equation model containing path coefficients and R2 values. The results of the assessment were satisfactory and support the validity of the proposed model. The findings indicate that perceived consequences comprising expected usefulness, expected social interaction and expected reputation have a significant effect on knowledge sharing behavior. Furthermore, the affect and facilitation conditions exhibit a positive influence on the behavior of the information security virtual communities. Contrary to our initial assumption, the social factor has an insignificant effect on the knowledge sharing behavior of security experts. This finding suggests that knowledge sharing in information security has positive consequences and can reduce information security risks.

6.5 Limitations and Future Research

The limitations of this study and recommendations for future research of it will be discussed below. Firstly, it is not completely clear whether or not the findings of this study can be generalized to all technicians and professionals of virtual communities. This is because this study's findings are restricted to knowledge sharing intention among a single particular professional group: information security professionals. Therefore, more research is needed to increase the generalizability of the findings of this research.

Secondly, the process of knowledge sharing in global virtual communities may be totally different from the knowledge sharing process in intra-organizational and inter-organizational setting. Hence, more studies are needed to investigate knowledge sharing determinants in intra-organizational and inter-organizational environment.

The third limitation concerns the sample. The sample of the study consists of active members of PVCs. Thus, it was not possible to get the perceptions and ideas of those individuals who do not take part in virtual communities anymore. Such individuals would provide different ideas about the determinants. In addition, the reasons why they have withdrawn from the PVC would provide invaluable and rich information for the administrators of virtual communities. Accordingly, the results of the study can only be used to elucidate the current knowledge of contributors concerning the knowledge sharing activities in virtual communities. A good area of research for future studies would be to investigate the reasons why some individuals either do not take part or have less active participation in information security virtual communities. Lastly, it has to be mentioned that this study has not examined the effects of moderating variables on the relationship between dependent and independent constructs. Therefore, future

researches must take into account moderating variables between dependent and independent constructs.

REFERENCES

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). Research report: the evolving relationship between general and specific computer self-efficacy—an empirical assessment. Information Systems Research, 11(4), 418-430.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior: Springer.

Ajzen, I. (2006). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. Journal of applied social psychology, 32(4), 665-683.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour.

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. Mis Quarterly, 107-136.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE Approach. Pittsburgh, PA, Carnegie Mellon University.

Al-Khaldi, M. A., & Olusegun Wallace, R. (1999). The influence of attitudes on personal computer utilization among knowledge workers: the case of Saudi Arabia. Information & Management, 36(4), 185-204.

Allison, P. (1999). Logistic regression using SAS®: theory and application. SAS Publishing.

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313.

Ardichvili, A., Maurer, M., Li, W., Wentling, T., & Stuedemann, R. (2006). Cultural influences on knowledge sharing through online communities of practice. Journal of knowledge management, 10(1), 94-107.

Ayoub, R. (2011). The 2011 (ISC) 2 Global Information Security Workforce Study. ISC2 (Ed.), 1-26.

Ba, S. (2001). Establishing online trust through a community responsibility system. Decision Support Systems, 31(3), 323-336.

Ba, S., Stallaert, J., & Whinston, A. B. (2001). Research commentary: introducing a third dimension in information systems design—the case for incentive alignment. Information Systems Research, 12(3), 225-239.

Baird, A., Jamieson, R., & Cerpa, N. (2003). Development of a Framework for Risks and Security in B2C E-Business Towards the Knowledge Society (pp. 399-413): Springer.

Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory: Prentice-Hall, Inc.

Bandura, A. (1997). Self-efficacy: The exercise of control: New York: Freeman.

Barab, S. A., MaKinster, J. G., & Scheckler, R. (2003). Designing system dualities: Characterizing a web-supported professional development community. The Information Society, 19(3), 237-256.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of personality and social psychology, 51(6), 1173.

Bartol, K. M., & Srivastava, A. (2002). Encouraging knowledge sharing: The role of organizational reward systems. Journal of Leadership & Organizational Studies, 9(1), 64-76.

Baskerville, R. (1988). Designing information systems security: John Wiley & Sons, Inc.

Baumeister, R. F., & Leary, M. R. (1995). The need to belong: desire for interpersonal attachments as a fundamental human motivation. Psychological bulletin, 117(3), 497.

Bergeron, F., Raymond, L., Rivard, S., & Gara, M.-F. (1995). Determinants of EIS use: Testing a behavioral model. Decision Support Systems, 14(2), 131-146.

Bieber, M., Engelbart, D., Furuta, R., Hiltz, S. R., Noll, J., Preece, J., Edward A. S., Turoff. M., Walle ,B.,Vand.E .(2002). Toward virtual community knowledge evolution. Journal of Management Information Systems, 18(4), 11-35.

Bifulco, A., & Santoro, R. (2005). A Conceptual Framework for "Professional Virtual Communities" Collaborative Networks and their Breeding Environments (pp. 417-424): Springer.

Blau, P. M. (1964). Exchange and power in social life: Transaction Publishers.

Bock, G. W., & Kim, Y.-G. (2002). Breaking the myths of rewards: an exploratory study of attitudes about knowledge sharing. Information Resources Management Journal (IRMJ), 15(2), 14-21.

Bock, G.-W., Zmud, R. W., Kim, Y.-G., & Lee, J.-N. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate. Mis Quarterly, 87-111.

Bock, G. W. G., & Kim, Y. G. (2003). Exploring the influence of rewards on attitudes towards knowledge sharing. Advanced topics in information resources management, 2, 220.

Boon, S. D., & Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. Cooperation and prosocial behavior, 190-211.

Bressler, S. E., & Grantham, C. (2000). Communities of commerce: Building internet business communities to accelerate growth, minimize risk, and increase customer loyalty: McGraw-Hill Professional.

Burnkrant, R. E., & Page Jr, T. J. (1982). An examination of the convergent, discriminant, and predictive validity of Fishbein's behavioral intention model. Journal of marketing research, 550-561.

Butler, B., Sproull, L., Kiesler, S., & Kraut, R. (2007). Community effort in online groups: Who does the work and why? Human-Computer Interaction Institute, 90.

Cabrera, E. F., & Cabrera, A. (2005). Fostering knowledge sharing through people management practices. The International Journal of Human Resource Management, 16(5), 720-735.

Carrillo, P., Robinson, H., Al-Ghassani, A., & Anumba, C. (2004). Knowledge management in UK construction: Strategies, resources and barriers. Project Management Journal, 35(1), 46-56.

Casimir, G., Ng, Y. N. K., & Cheng, C. L. P. (2012). Using IT to share knowledge and the TRA. Journal of knowledge management, 16(3), 461-479.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70-104.

Center for Strategic and International Studies (CSIS). (2009). Significant cyber events since 2006. Retrieved 22 December 2009 from http://csis.org/files/publication/091109_cyber_events_since_2006.pdf

Chan, C. K. K., & Chan, Y. Y. (2011). Students' views of collaboration and online participation in Knowledge Forum. Computers & Education, 57(1), 1445-1457.

Chang, H. H., & Chuang, S. S. (2011). Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator. Information & Management, 48(1), 9-18.

Chang, M. K., & Cheung, W. (2001). Determinants of the intention to use Internet/WWW at work: a confirmatory study. Information & Management, 39(1), 1-14.

Chang, M. K., Cheung, W., & Lai, V. S. (2005). Literature derived reference models for the adoption of online shopping. Information & Management, 42(4), 543-559.

Chen, C.-J., & Hung, S.-W. (2010). To give or to receive? Factors influencing members' knowledge sharing and community promotion in professional virtual communities. Information & Management, 47(4), 226-236.

Chen, I. Y. (2007). The factors influencing members' continuance intentions in professional virtual communities—a longitudinal study. Journal of Information Science, 33(4), 451-467.

Chen, I. Y., & Chen, N.-S. (2009). Examining the Factors Influencing Participants' Knowledge Sharing Behavior in Virtual Learning Communities. Educational Technology & Society, 12(1), 134-148.

Chen, J. Q., Schmidt, M. B., Phan, D. D., & Arnett, K. P. (2008). E-commerce security threats: awareness, trust and practice. International Journal of Information Systems and Change Management, 3(1), 16-32.

Chen, S.-S., Chuang, Y.-W., & Chen, P.-Y. (2012). Behavioral intention formation in knowledge sharing: Examining the roles of KMS quality, KMS self-efficacy, and organizational climate. Knowledge-Based Systems, 31, 106-118.

Chen, Y.-J., & Chen, Y.-M. (2012). Knowledge evolution course discovery in a professional virtual community. Knowledge-Based Systems, 33(0), 1-28. doi: http://dx.doi.org/10.1016/j.knosys.2012.02.016

Cheung, W., Chang, M. K., & Lai, V. S. (2000). Prediction of Internet and World Wide Web usage at work: a test of an extended Triandis model. Decision Support Systems, 30(1), 83-100.

Chin, W. W. (1998). The partial least squares approach for structural equation modeling.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. Information Systems Research, 14(2), 189-217.

Chin, W. W., & Newsted, P. R. (1999). Structural equation modeling analysis with small samples using partial least squares. Statistical strategies for small sample research, 1(1), 307-341.

Chiu, C.-M., Hsu, M.-H., & Wang, E. T. (2006). Understanding knowledge sharing in virtual communities: an integration of social capital and social cognitive theories. Decision Support Systems, 42(3), 1872-1888.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals in organizational knowledge sharing. Information & Management, 45(7), 458-465.

Chu, S. K. W., Chan, C. K. K., & Tiwari, A. F. Y. (2012). Using blogs to support learning during internship. Computers & Education, 58(3), 989-1000.

Coleman, J. S. (1988). Social capital in the creation of human capital. American journal of sociology, 95-120.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. Mis Quarterly, 189-211.

Constant, D., Kiesler, S., & Sproull, L. (1994). What's mine is ours, or is it? A study of attitudes about information sharing. Information Systems Research, 5(4), 400-421.

Consulting, A. A. B. (1999). Zukai knowledge management. Tokyo: Toyo Keizai.

Conti, G. (2005). Why computer scientists should attend hacker conferences. Communications of the ACM, 48(3), 23-24.

Cowan, D. D., Mayfield, C. I., Tompa, F. W., & Gasparini, W. (1998). New role for community networks. Communications of the ACM, 41(4), 61-63.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012). Future Directions for Behavioral Information Security Research. Computers & Security.

Yazar, Z. (2002). A qualitative risk analysis and management tool–CRAMM. SANS InfoSec Reading Room White Paper.

Davenport, T. H., De Long, D. W., & Beers, M. C. (1998). Successful knowledge management projects. Sloan management review, 39(2), 43-57.

Davenport, T. H., & Pruzak, L. (2000). Working knowledge: How organizations manage what they know: Harvard Business Press.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. Management Science, 35(8), 982-1003.

Dempsey, K. (2011). Information Security Continuous Monitoring (ISCM) for Federal Systems and Organisations. Nist special publication, 800-137.

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. Organization science, 5(2), 121-147.

Detlor, B. (2002). An informational perspective towards knowledge work: Implications for knowledge management systems. Knowledge Mapping and Management. Hershey, 195-205.

Dlamini, M., Eloff, J. H. P., & Eloff, M. (2009). Information security: The moving target. Computers & Security, 28(3), 189-198.

Donath, J. S. (1999). Identity and deception in the virtual community. Communities in cyberspace, 1996, 29-59.

Du, R., Ai, S., & Ren, Y. (2007). Relationship between knowledge sharing and performance: A survey in Xi'an, China. Expert Systems with Applications, 32(1), 38-46.

Dunkerley, K. D., & Adviser-Tejay, G. (2011). Developing an information systems security success model for organizational context.

Earl, M. (2012). Experiences in strategic information systems planning. Strategic Information Management, 181.

Edwards, J. R. (2001). Multidimensional constructs in organizational behavior research: An integrative analytical framework. Organizational Research Methods, 4(2), 144-192.

Eloff, M. M., & Von Solms, S. (2000). Information security management: a hierarchical framework for various approaches. Computers & Security, 19(3), 243-256.

Endler, D., & Collier, M. (2007). Hacking Exposed VoIP: Tata McGraw-Hill Education.

Endres, M. L., Endres, S. P., Chowdhury, S. K., & Alam, I. (2007). Tacit knowledge sharing, self-efficacy theory, and application to the Open Source community. Journal of knowledge management, 11(3), 92-103.

Fahey, L., & Prusak, L. (1998). The eleven deadliest sins of knowledge management. California management review, 40(3), 265.

Fang, Y. H., & Chiu, C. M. (2010). In justice we trust: Exploring knowledge sharing continuance intentions in virtual communities of practice. Computers in Human Behavior, 26(2), 235-246.

Fehr, E., & Gächter, S. (2000). Fairness and retaliation: The economics of reciprocity.

Feledi, D., & Fenz, S. (2012). Challenges of Web-Based Information Security Knowledge Sharing. Paper presented at the Availability, Reliability and Security (ARES), 2012 Seventh International Conference on.

Feledi, D., Fenz, S., & Lechner, L. (2013). Toward web-based information security knowledge sharing. Information security technical report.

Fenz, S., & Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. Security & Privacy, IEEE, 9(2), 58-65.

Fenz, S., Parkin, S., & van Moorsel, A. (2011). A Community Knowledge Base for IT Security. IT Professional, 13(3), 24-30.

Fernback, J. (1999). There is a there there: Notes toward a definition of cybercommunity. Doing Internet research: Critical issues and methods for examining the Net, 203-220.

Finin, T., Joshi, A., Kargupta, H., Yesha, Y., Sachs, J., Bertino, E., Ninghui, L.,Thuraisingham, B. (2009). Assured information sharing life cycle. Paper presented at the Intelligence and Security Informatics, 2009. ISI'09. IEEE International Conference on.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research.

Fidell, L. S., & Tabachnick, B. G. (2006). Using multivariate statistics. Boston: Allyn & Bacon.

Ford, D. P. (2005). Knowledge sharing: Seeking to understand intentions and actual sharing.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of marketing research, 382-388.

Forstenlechner, I., & Lettice, F. (2007). Cultural differences in motivating global knowledge workers. Equal Opportunities International, 26(8), 823-833.

French Jr, J. R., & Raven, B. (1959). The bases of social power.

Furnell, S., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410-417.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186-208.

Garud, R., & Kumaraswamy, A. (2005). Vicious and virtuous circles in the management of knowledge: The case of Infosys Technologies. Mis Quarterly, 9-33.

Gecas, V. (1989). The social psychology of self-efficacy. Annual review of sociology, 291-316.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. Mis Quarterly, 51-90.

Gefen, D., Straub, D. W., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice.

Gongla, P., & Rizzuto, C. R. (2001). Evolving communities of practice: IBM Global Services experience. IBM systems journal, 40(4), 842-862.

Goodhue, D. (1988). I/S attitudes: toward theoretical and definitional clarity. ACM SIGMIS Database, 19(3-4), 6-15.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 22(6), 461-485.

Gordon, S. (1995). Internet 101. Computers & Security, 14(7), 599-604.

Granovetter, M. S. (1973). The strength of weak ties. American journal of sociology, 1360-1380.

Gupta, A. K., & Govindarajan, V. (2000). Knowledge flows within multinational corporations. Strategic Management Journal, 21(4), 473-496.

Gupta, M., Walp, J., & Sharman, R. (2012). Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions: Information Science Reference.

Haas, M. R., & Hansen, M. T. (2007). Different knowledge, different benefits: toward a productivity perspective on knowledge sharing in organizations. Strategic Management Journal, 28(11), 1133-1153.

Hagel, J. (1999). Net gain: expanding markets through virtual communities. Journal of Interactive Marketing, 13(1), 55-65.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate analysis. Englewood: Prentice Hall International.

Hair Jr, J. F., Anderson, R. E., & Tatham, R. L. (1986). Multivariate data analysis with readings: Macmillan Publishing Co., Inc.

Hamill, J. T., Deckro, R. F., & Kloeber Jr, J. M. (2005). Evaluating information assurance strategies. Decision Support Systems, 39(3), 463-484.

Hasan, B. (2006). Delineating the effects of general and system-specific computer self-efficacy beliefs on IS acceptance. Information & Management, 43(5), 565-571.

He, J. (2009). EXAMINING FACTORS THAT AFFECT KNOWLEDGE SHARING AND STUDENTS'ATTITUDE TOWARD THEIR LEARNING EXPERIENCE WITHIN VIRTUAL TEAMS. University of Central Florida Orlando, Florida.

He, J., & Freeman, L. A. (2010). Understanding the formation of general computer self-efficacy. Communications of the Association for Information Systems, 26(1), 12.

He, W., & Wei, K. K. (2009). What drives continued knowledge sharing? An investigation of knowledge-contribution and-seeking beliefs. Decision Support Systems, 46(4), 826-838.

Heinze, N., & Hu, Q. (2009). Why college undergraduates choose IT: a multi-theoretical perspective. European Journal of Information Systems, 18(5), 462-475.

Hew, K. F., & Hara, N. (2007). Knowledge sharing in online environments: A qualitative case study. Journal of the American Society for Information Science and Technology, 58(14), 2310-2324.

Ho, R. (2006). Handbook of univariate and multivariate data analysis and interpretation with SPSS: Chapman & Hall/CRC.

Holsapple, C. W., & Joshi, K. D. (2004). A formal knowledge management ontology: Conduct, activities, resources, and influences. Journal of the American Society for Information Science and Technology, 55(7), 593-612.

Holtshouse, D. (1998). Knowledge research issues. California management review, 40(3), 277.

Hong, J. F., & Vai, S. (2008). Knowledge sharing in cross-functional virtual teams. Journal of General Management, 34(2), 21.

Horng, S. J., Su, M. Y., Chen, Y. H., Kao, T. W., Chen, R. J., Lai, J. L., & Perkasa, C. D. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert Systems with Applications, 38(1), 306-313.

Horrigan, J. B., & Rainie, L. (2006). The Internet's growing role in life's major moments (Vol. 181): Pew Internet & American Life Project Washington, DC.

Hsu, C.-L., & Lin, J. C.-C. (2008). Acceptance of blog usage: The roles of technology acceptance, social influence and knowledge sharing motivation. Information & Management, 45(1), 65-74.

Hsu, M.-H., Ju, T. L., Yen, C.-H., & Chang, C.-M. (2007). Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. International Journal of Human-Computer Studies, 65(2), 153-169.

Hu, P. J.-H., Clark, T. H., & Ma, W. W. (2003). Examining technology acceptance by school teachers: a longitudinal study. Information & Management, 41(2), 227-241.

Huang, C. C. (2009). Knowledge sharing and group cohesiveness on performance: An empirical study of technology R&D teams in Taiwan. Technovation, 29(11), 786-797.

Huber, G. P. (1991). Organizational learning: The contributing processes and the literatures. Organization science, 2(1), 88-115.

Hult, G. T. M., Ketchen, D. J., & Nichols, E. L. (2002). An examination of cultural competitiveness and order fulfillment cycle time within supply chains. Academy of management Journal, 45(3), 577-586.

Humphreys, T. (2006). State-of-the-art information security management system with ISO/IEC 27001, ISO Management Systems (Special Report), 9-13.

Hung, S.-W., & Cheng, M.-J. (2012). Are you ready for knowledge sharing? An empirical study of virtual communities. Computers & Education.

Hung, S.-Y., Durcikova, A., Lai, H.-M., & Lin, W.-M. (2011). The influence of intrinsic and extrinsic motivation on individuals' knowledge sharing behavior. International Journal of Human-Computer Studies, 69(6), 415-427.

Igbaria, M., Iivari, J., & Maragahh, H. (1995). Why do individuals use computer technology? A Finnish case study. Information & Management, 29(5), 227-238.

Initiative, J. T. F. T. (2011). SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View.

Isaca. (2010). CISA review manual 2010: Isaca. Retrieved June 14, 2013, from http://www.isaca.org/ COBIT/ Documents/ COBIT-5-for-Information-Security Introduction.pdf

ISO 17799 (2000). ISO/IEC 17799:2000. Information technology - code of practice for information security management, International Organization for Standardization.

ISO/IEC 27005:2008, Information technology, Security techniques Information security risk management, International Standards Organization

Jansen, W. (2010). Directions in security metrics research: DIANE Publishing.

Jeon, S., Kim, Y.-G., & Koh, J. (2011). An integrative model for knowledge sharing in communities-of-practice. Journal of knowledge management, 15(2), 251-269.

Jeon, S.-H., Kim, Y.-G., & Koh, J. (2011). Individual, social, and organizational contexts for active knowledge sharing in communities of practice. Expert Systems with Applications, 38(10), 12423-12431.

Johnson, C. A. (2007). Social capital and the search for information: Examining the role of social capital in information seeking behavior in Mongolia. Journal of the American Society for Information Science and Technology, 58(6), 883-894.

Johnson, D. W., & Johnson, R. T. (1987). Learning together and alone: Cooperative, competitive, and individualistic learning: Prentice-Hall, Inc.

Jonassen, D., Davidson, M., Collins, M., Campbell, J., & Haag, B. B. (1995). Constructivism and computer-mediated communication in distance education. American journal of distance education, 9(2), 7-26.

Kagal, L., Finin, T., & Joshi, A. (2001). Trust-based security in pervasive computing environments. Computer, 34(12), 154-157.

Kagal, L., Finin, T., & Joshi, A. (2003). A policy based approach to security for the semantic web The Semantic Web-ISWC 2003 (pp. 402-418): Springer.

Kankanhalli, A., Tan, B. C. Y., & Wei, K. K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. Mis Quarterly, 113-143.

Kesh, S., & Ratnasingam, P. (2007). A knowledge architecture for IT security. Communications of the ACM, 50(7), 103-108.

Kim, Y., & Ahmad, M. A. (2012). Trust, distrust and lack of confidence of users in online social media-sharing communities. Knowledge-Based Systems.

King, C., Dalton, C., & Osmanoglu, T. (2001). Security Architecture-Design, Development & Operations, Business and Application Drivers (Case Study): McGraw-Hill/Osborne.

Klang, M., & Olsson, S. (1999). Virtual communities. Paper presented at the Proceedings of the 22 nd Information Systems Research Seminar in Scandinavia.

Kogut, B., & Zander, U. (1992). Knowledge of the firm, combinative capabilities, and the replication of technology. Organization science, 3(3), 383-397.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597-607.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. Computers & Security, 27(5), 224-231.

Kuo, F.-Y., & Young, M.-L. (2008). Predicting knowledge sharing practices through intention: A test of competing models. Computers in Human Behavior, 24(6), 2697-2722.

Lam, A. (2000). Tacit knowledge, organizational learning and societal institutions: an integrated framework. Organization studies, 21(3), 487-513.

Landau, S., & Everitt, B. S. (2003). A handbook of statistical analyses using SPSS: Chapman & Hall/CRC.

Lander, M. C., Purvis, R. L., McCray, G. E., & Leigh, W. (2004). Trust-building mechanisms utilized in outsourced IS development projects: a case study. Information & Management, 41(4), 509-528.

Larson, A. (1992). Network dyads in entrepreneurial settings: A study of the governance of exchange relationships. Administrative Science Quarterly, 76-104.

Lee, D.-J., & Ahn, J.-H. (2007). Reward systems for intra-organizational knowledge sharing. European Journal of Operational Research, 180(2), 938-956.

Lee, F. S., Vogel, D., & Limayem, M. (2002). Virtual community informatics: what we know and what we need to know. Paper presented at the System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on.

Lee, F. S. L., Vogel, D., & Limayem, M. (2003). Virtual community informatics: A review and research agenda. Journal of Information Technology Theory and Application (JITTA), 5(1), 5.

Lee, J.-N. (2001). The impact of knowledge sharing, organizational capability and partnership quality on IS outsourcing success. Information & Management, 38(5), 323-335.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. Commun. ACM, 48(8), 72-77. doi: 10.1145/1076211.1076243

Lesser, E. L., & Storck, J. (2001). Communities of practice and organizational performance. IBM systems journal, 40(4), 831-841.

Li, W. (2010). Virtual knowledge sharing in a cross-cultural context. Journal of knowledge management, 14(1), 38-50.

Liao, L.-F. (2006). The impact of teacher's powers to knowledge sharing behavior and learning satisfaction in distance-learning environment. Journal of Information, Technology and Society, 2(3), 1-14.

Lichtenstein, S. (1998). Internet risks for companies. Computers & Security, 17(2), 143-150.

Lichtenstein, S., & Hunter, A. (2004). Considering the receiver in knowledge sharing: When the receiver seems ready the sharer appears. Paper presented at the ACKMIDS 2004: Organisational challenges for knowledge management Proceedings of the Australian Conference on Knowledge Management and Intelligent Decision Support.

Lin, F.-r., Lin, S.-c., & Huang, T.-p. (2008). Knowledge sharing and creation in a teachers' professional virtual community. Computers & Education, 50(3), 742-756.

Lin, H.-F. (2007). Knowledge sharing and firm innovation capability: an empirical study. International Journal of Manpower, 28(3/4), 315-332.

Lin, M.-J. J., Hung, S.-W., & Chen, C.-J. (2009). Fostering the determinants of knowledge sharing in professional virtual communities. Computers in Human Behavior, 25(4), 929-939.

Lin, T.-C., Wu, S., & Lu, C.-T. (2012). Exploring the affect factors of knowledge sharing behavior: The relations model theory perspective. Expert Systems with Applications, 39(1), 751-764.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. Decision Support Systems, 52(1), 95-107.

Liu, P., Raahemi, B., & Benyoucef, M. (2011). Knowledge sharing in dynamic virtual enterprises: a socio-technological perspective. Knowledge-Based Systems, 24(3), 427-443.

Liu, W., Tanaka, H., & Matsuura, K. (2006). An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan. Paper presented at the WEIS.

Loch, K. D., & Conger, S. (1996). Evaluating ethical decision making and computer use. Commun. ACM, 39(7), 74-83. doi: 10.1145/233977.233999

Lohmöller, J.-B. (1989). Latent variable path modeling with partial least squares: Physica-Verlag Heidelberg.

Luarn, P., & Lin, H. H. (2005). Toward an understanding of the behavioral intention to use mobile banking. Computers in Human Behavior, 21(6), 873-891.

Lucas Jr, H. C. (1978). Empirical evidence for a descriptive model of implementation. Mis Quarterly, 27-42.

Ma, M., & Agarwal, R. (2007). Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities. Information Systems Research, 18(1), 42-67.

Ma, W. W. K., & Yuen, A. H. K. (2011). Understanding online knowledge sharing: An interpersonal relationship perspective. Computers & Education, 56(1), 210-219.

Machlup, F. (1980). Knowledge: Its creation, distribution, and economic significance (Vol. 1): Princeton University Press Princeton, NJ.

Majchrzak, A., Rice, R. E., Malhotra, A., King, N., & Ba, S. (2000). Technology adaption: the case of a computer-supported inter-organizational virtual team 1. Mis Quarterly, 24(4), 569-600.

Marett, K., & Joshi, K. (2009). The decision to share information and rumors: examining the role of motivation in an online discussion forum. Communications of the Association for Information Systems, 24(1), 4.

Matzler, K., Renzl, B., Müller, J., Herting, S., & Mooradian, T. A. (2008). Personality traits and knowledge sharing. Journal of Economic Psychology, 29(3), 301-313.

Mayer, A., Wool, A., & Ziskind, E. (2000). Fang: A firewall analysis engine. Paper presented at the Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on.

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. Academy of management Journal, 24-59.

McDonagh, J., & Harbison, A. (2000). Behind the Celtic Tiger: Key Issues in the Management of Information Technology in. Paper presented at the Challenges of Information Technology Management in the 21st Century: 2000 Information Resources Management Association International Conference, Anchorage, Alaska, USA, May 21-24, 2000.

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2006). Anchoring information security governance research: Sociological groundings and future directions. Journal of Information Systems Security, 2(3), 3-47.

McLure Wasko, M., & Faraj, S. (2000). "It is what one does": why people participate and help others in electronic communities of practice. The Journal of Strategic Information Systems, 9(2), 155-173.

Meyers, L. S., Gamst, G., & Guarino, A. J. (2006). Applied multivariate research: Design and interpretation. Sage.

Microsoft, 2006,The Security Risk Management Guide. Retrieved July 15, 2013,from http://www.microsoft.com/en-us/download/details.aspx?id=6232

Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. Academy of management review, 23(2), 242-266.

Nakashima, E. (2009, Dec 19). Encryption of drone feeds won't finish until 2014, Air Force says. Retrieved 22 December 2009 from http://www.washingtonpost.com/wp-dyn/content/article/2009/12/18/AR2009121804281.html

Nelson, K. M., & Cooprider, J. G. (1996). The contribution of shared knowledge to IS group performance. Management Information Systems Quarterly, 20, 409-432.

NIST, S. (2002). 800-30. Risk management guide for information technology systems, 800-830.

Nnolim, A. L. (2007). A framework and methodology for information security management: ProQuest.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. Organization science, 5(1), 14-37.

Official Google Blog: A New Approach to China(2010). Retrieved January 12, 2010, from http://googleblog.blogspot.com /2010/01/new-approach-to-china.html

Pabrai, U. O., & Gurbani, V. K. (1996). Internet TCP/IP Network Security: Securing Protocols and Applications: McGraw-Hill, Inc.

Pai, J.-C. (2006). An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP). Management Decision, 44(1), 105-122.

Panteli, N., & Sockalingam, S. (2005). Trust and conflict within virtual inter-organizational alliances: a framework for facilitating knowledge sharing. Decision Support Systems, 39(4), 599-617.

Pare, G., & Elam, J. J. (1995). Discretionary use of personal computers by knowledge workers: testing of a social psychology theoretical model. Behaviour & Information Technology, 14(4), 215-228.

Paroutis, S., & Al Saleh, A. (2009). Determinants of knowledge sharing using Web 2.0 technologies. Journal of knowledge management, 13(4), 52-63.

Peddibhotla, N. B., & Subramani, M. R. (2007). Contributing to public document repositories: A critical mass theory perspective. Organization studies, 28(3), 327-346.

Pegrum, M. S., Jamieson, D., & Yuen, M. (2003). Virtual private networks: Google Patents.

Peltier, T. R. (2005). Information security risk analysis: Auerbach Publications.

Piaget, J. (1965). The Moral Judgment of the Child.(Translated by Marjorie Gabain): Routledge & K. Paul.

Pietro, R., & Mancini, L. V. (2008). Intrusion Detection Systems: Springer.

Polanyi, M. (1962). Personal knowledge: Towards a post-critical philosophy: Psychology Press.

Porter, L. W., & Lawler, E. E. (1968). Managerial attitudes and performance: RD Irwin Homewood, IL.

Potter, C., & Beard, A. (2010). Information Security Breaches Survey 2010. Price Water House Coopers. Earl's Court, London.

Ratnasingam, P. (2005). Trust in inter-organizational exchanges: a case study in business to business electronic commerce. Decision Support Systems, 39(3), 525-544.

Ratnasingam, P., & Pavlou, P. (2002). Technology trust: the next value creator in B2B electronic commerce. Paper presented at the Information Resources Management Association International Conference.

Richardson, R. (2011). 15th annual 2010/2011 computer crime and security survey. Computer Security Institute, New York, NY.

Richardson, R. (2011). 2010/2011 Computer Crime and Security Survey. Computer Security Institute. Available at: http://analytics. informationweek. com/abstract/21/7377/Security/research-2010-2011-csisurvey. html (Accessed: 14 July 2011).

Richardson, R. (2011). 2011 CSI Computer Crime and Security Survey.". Computer Security Institute.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. The Journal of Strategic Information Systems, 11(3), 271-295.

Ring, P. S., & Van de Ven, A. H. (1994). Developmental processes of cooperative interorganizational relationships. Academy of management review, 19(1), 90-118.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0 (M3) Beta. Retrieved August 22, 2012, from http://www. smartpls. de.

Ross, R., Katzke, S., Johnson, A., Swanson, M., & Stoneburner, G. (2008). NIST SP800-39, Managing Risk from Information Systems An Organizational Perspective: Gaithersberg, MD: NIST, http://csrc. nist. gov/publications/drafts/800-39/SP800-39-spd-sz. pdf.

Ryu, S., Ho, S. H., & Han, I. (2003). Knowledge sharing behavior of physicians in hospitals. Expert Systems with Applications, 25(1), 113-122.

Saadé, R., & Bahli, B. (2005). The impact of cognitive absorption on perceived usefulness and perceived ease of use in on-line learning: an extension of the technology acceptance model. Information & Management, 42(2), 317-327.

Saadé, R. G., & Kira, D. (2009). Computer anxiety in e-learning: The effect of computer self-efficacy. Journal of Information Technology Education, 8, 177-191.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal, 39(4), 60-66.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. Communications Magazine, IEEE, 32(9), 40-48.

Santoro, R., & Bifulco, A. (2008). Professional virtual communities reference framework Methods and Tools for Collaborative Networked Organizations (pp. 277-294): Springer.

Scambray, J., McClure, S., & Kurtz, G. (2001). Hacking Exposed, Osborne: McGraw-Hill.

Schultz, R. L., & Slevin, D. P. (1973). Implementation and organizational validity: An empirical investigation: Institute for Research in the Behavioral, Economic, and Management Sciences, Purdue University.

Schultze, U. (2000). A confessional account of an ethnography about knowledge work. Mis Quarterly, 3-41.

Singh, A. (2009). Improving Information Security Risk Management. UNIVERSITY OF MINNESOTA.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.

Sole, D., & Edmondson, A. (2002). Situated knowledge and learning in dispersed teams. British Journal of Management, 13(S2), S17-S34.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.

Stone, R. W., & Henry, J. W. (2002). The Roles of Computer Self-Efficacy and Outcome Expectancy in Influencing the Computer End-User's Organizational. Advanced topics in end user computing, 2, 44.

Steenkamp, A. L., & McCord, S. A. (2006), Doctoral Research Prospectus, Lawrence Technological University, Southfield, Michigan.

Szymanski, D. M., & Hise, R. T. (2000). E-satisfaction: an initial examination. Journal of retailing, 76(3), 309-322.

Tamjidyamcholo, A. (2012). Information security risk reduction based on genetic algorithm. Paper presented at the Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on.

Tamjidyamcholo, A., & Al-Dabbagh, R. D. (2012). Genetic Algorithm Approach for Risk Reduction of Information Security. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1(1), 59-66.

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H., & Gholipour, R. (2013). Information security–professional perceptions of knowledge sharing intention under self-efficacy, trust, reciprocity, and shared-language. Computers & Education.

Teo, H. H., Chan, H. C., Wei, K. K., & Zhang, Z. (2003). Evaluating information accessibility and community adaptivity features for sustaining virtual learning communities. International Journal of Human-Computer Studies, 59(5), 671-697.

Teo, T. S., Lim, V. K., & Lai, R. Y. (1999). Intrinsic and extrinsic motivation in Internet usage. Omega, 27(1), 25-37.

Thatcher, J. B., & Perrewe, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. Mis Quarterly, 381-396.

Thibaut, J. W., & Kelley, H. H. (1959). The social psychology of groups.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: toward a conceptual model of utilization. Mis Quarterly, 125-143.

Tipton, H. F., & Henry, K. (2006). Official (ISC) 2 guide to the CISSP CBK: Auerbach Publications.

Tiwana, A. (1999). Are Firewalls Enough: Web Security, Digital Press.

Tiwana, A., & Mclean, E. R. (2003). Expertise integration and creativity in information systems development. Journal of Management Information Systems, 22(1), 13-43.

Tönnies, F. (1955). Community and association:(Gemeinschaft und gesellschaft): Routledge & Paul.

Triandis, H. (1980). Beliefs, attitudes, and values. Paper presented at the Nebraska symposium on motivation.

Triandis, H. C. (1971). Attitude and attitude change: Wiley New York.

Triandis, H. C. (1979). Values, attitudes, and interpersonal behavior. Paper presented at the Nebraska symposium on motivation.

Tsai, M.-T., & Cheng, N.-C. (2010). Programmer perceptions of knowledge sharing behavior under social cognitive theory. Expert Systems with Applications, 37(12), 8479-8485. doi: http://dx.doi.org/10.1016/j.eswa.2010.05.029

Tsai, W. (2002). Social structure of "coopetition" within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. Organization science, 13(2), 179-190.

Tsai, W., & Ghoshal, S. (1998). Social capital and value creation: The role of intrafirm networks. Academy of management Journal, 41(4), 464-476.

Tuomi, I. (1999). Data is more than knowledge: implications of the reversed knowledge hierarchy for knowledge management and organizational memory. Paper presented at the System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. Management Science, 46(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. Mis Quarterly, 425-478.

Venkateswaran, R. (2001). Virtual private networks. Potentials, IEEE, 20(1), 11-15.

Venter, H., & Eloff, J. H. P. (2003). A taxonomy for information security technologies. Computers & Security, 22(4), 299-307.

Vermeulen, C., & Von Solms, R. (2002). The information security management toolbox–taking the pain out of security management. Information management & computer security, 10(3), 119-125.

Vijayasarathy, L. R. (2004). Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model. Information & Management, 41(6), 747-762.

von Solms, B. (2006). Information security–the fourth wave. Computers & Security, 25(3), 165-168.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.

Vroom, V. H. (1964). Work and motivation.

Wasko, M. M. L., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. Mis Quarterly, 35-57.

Wenger, E. (1998). Communities of practice: Learning, meaning, and identity: Cambridge university press.

Wheeler, E. (2011). Security risk management. Syngress, Waltham, MA.

Whitman, M. E., & Mattord, H. J. (2010). The enemy is still at the gates: threats to information security revisited. Paper presented at the 2010 Information Security Curriculum Development Conference.

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security: Course Technology Ptr.

Whitman, M. E., Mattord, H. J., Austin, R., & Holden, G. (2009). Guide to Firewalls and Network Security: Intrusion Detection and VPNS: Course Technology/Cengage Learning.

Wijnhoven, F. (1998). Knowledge logistics in business contexts: analyzing and diagnosing knowledge sharing by logistics concepts. Knowledge and Process Management, 5(3), 143-157.

Wikström, S., Normann, R., Anell, B., Ekvall, G., Forslin, J., & Skärvad, P.-H. (1994). Knowledge and value: A new perspective on corporate transformation (Vol. 35): Routledge London.

Wu, H.-H., & Wei, C.-W. (2010). Factors affecting learners' knowledge sharing intentions in web-based learning. Paper presented at the Computer Communication Control and Automation (3CA), 2010 International Symposium on.

Xiao-qing, B., Qing-xiang, Z., & Mang, Y. (2010). The identification method of the risk factors of knowledge sharing based on the evidence theory. Paper presented at the Advanced Management Science (ICAMS), 2010 IEEE International Conference on.

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. Government Information Quarterly, 28(2), 164-175.

Yli-Renko, H., Autio, E., & Sapienza, H. J. (2001). Social capital, knowledge acquisition, and knowledge exploitation in young technology-based firms. Strategic Management Journal, 22(6-7), 587-613.

Zboralski, K. (2009). Antecedents of knowledge sharing in communities of practice. Journal of knowledge management, 13(3), 90-101.

Zolfaghar, K., & Aghaie, A. (2012). A syntactical approach for interpersonal trust prediction in social web applications: Combining contextual and structural data. Knowledge-Based Systems, 26, 93-102.