THREE ESSAYS ON INFORMATION SECURITY RISK MANAGEMENT

Obiageli Ogbanufe

Dissertation Prepared for the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

May 2018

APPROVED:

Dan J. Kim, Committee Chair
Nick Evangelopoulos, Committee Member
Robert Pavur, Committee Member
Raghav Rao, Committee Member
Leon Kappelman, Department of Information Technology and Decision Sciences
Marilyn Wiley, Dean of the College of Business
Victor Prybutok, Dean of the Toulouse Graduate School

Ogbanufe, Obiageli. *Three Essays on Information Security Risk Management*. Doctor of Philosophy (Business), May 2018, 169 pp., 20 tables, 8 figures, references, 324 titles.

Today’s environment is filled with the proliferation of cyber-attacks that result in losses for organizations and individuals. Hackers often use compromised websites to distribute malware, making it difficult for individuals to detect. The impact of clicking through a link on the Internet that is malware infected can result in consequences such as private information theft and identity theft. Hackers are also known to perpetrate cyber-attacks that result in organizational security breaches that adversely affect organizations’ finances, reputation, and market value. Risk management approaches for minimizing and recovering from cyber-attack losses and preventing further cyber-attacks are gaining more importance. Many studies exist that have increased our understanding of how individuals and organizations are motivated to reduce or avoid the risks of security breaches and cyber-attacks using safeguard mechanisms. The safeguards are sometimes technical in nature, such as intrusion detection software and anti-virus software. Other times, the safeguards are procedural in nature such as security policy adherence and security awareness and training. Many of these safeguards fall under the risk mitigation and risk avoidance aspects of risk management, and do not address other aspects of risk management, such as risk transfer. Researchers have argued that technological approaches to security risks are rarely sufficient for providing an overall protection of information system assets. Moreover, others argue that an overall protection must include a risk transfer strategy. Hence, there is a need to understand the risk transfer approach for managing information security risks. Further, in order to effectively address the information security puzzle, there also needs to be an understanding of the nature of the perpetrators of the problem – the hackers. Though hacker incidents proliferate the news, there are few theory based hacker studies. Even though the very nature of their actions presents a

difficulty in their accessibility to research, a glimpse of how hackers perpetrate attacks can be obtained through the examination of their knowledge sharing behavior. Gaining some understanding about hackers through their knowledge sharing behavior may help researchers fine-tune future information security research. The insights could also help practitioners design more effective defensive security strategies and risk management efforts aimed at protecting information systems. Hence, this dissertation is interested in understanding the hackers that perpetrate cyber-attacks on individuals and organizations through their knowledge sharing behavior. Then, of interest also is how individuals form their URL click-through intention in the face of proliferated cyber risks. Finally, we explore how and why organizations that are faced with the risk of security breaches, commit to cyberinsurance as a risk management strategy. Thus, the fundamental research question of this dissertation is: how do individuals and organizations manage information security risks?

ACKNOWLEDGMENTS

This dissertation marks the culmination of an important milestone in my life’s journey. I am thankful that several people have helped along the way and that I am not on this journey by myself. I would first like to thank my dissertation chair, Dan J. Kim. His guidance has been instrumental in the development of this dissertation. I would also like to thank my dissertation committee members; Drs. Nick Evangelopoulos, Robert Pavur, and H. Raghav Rao. They were generous with their time and added insights that improved the quality of my dissertation. I would like to thank my family for their unwavering support throughout the four years of my Ph.D program. I thank my husband, Chris, who encouraged and supported me all the way. I also recognize my children, Chinedu and Uzo for their support. I could not ask for better children.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

PROLOGUE

Today's environment is filled with the proliferation of cyber-attacks and security breaches that result in the subsequent losses that organizations and individuals suffer. The ability to manage those risks is becoming an important approach for not only minimizing and recovering from the loss of damage, but also for helping prevent further cyber-attacks. Hackers often use compromised or legitimately looking fake websites to distribute malware, making it difficult for individuals to detect (Abbasi, Zhang, Zimbra, Chen, & Nunamaker Jr, 2010). The impact of clicking through a link on the Internet that is malware infected can wreak havoc for the individual, including the stealing of private information (Dinev, 2006) and storing of surveillance software on individuals' computers in order to observe their behavior (Grazioli & Jarvenpaa, 2000).

Hackers are also known to perpetrate cyber-attacks that result in organizational security breaches. A security breach refers to the compromise of security, confidentiality, or integrity of, or loss of data that result in the unauthorized acquisition of sensitive data, applications, services, and networks. Security breaches have adversely affected organizations' reputation and market value (Cavusoglu et al. 2004; Mukhopadhyay et al. 2013). A survey of 2,000 consumers found that nearly 87 percent are unlikely to do business with organizations impacted by security breach (NCI 2016). Many studies exist that have increased our understanding of how individuals and organizations are motivated to reduce or avoid the risks of security breaches and cyber-attacks using safeguards. The safeguards are sometimes technical in nature, such as intrusion detection software and anti-virus software (Lee and Larsen 2009; Mookerjee et al. 2011). Other times, the safeguards are in the form of procedural safeguards such as security policy adherence and security training and awareness (e.g., Boss et al. 2015; Herath and Rao 2009a; Posey et al. 2015). These safeguards fall under the risk mitigation and risk avoidance aspects of risk management, and do not address the risk transfer aspect of risk management. Researchers have argued that technological approaches to security risks are rarely sufficient for providing an overall protection of IS assets (Herath and Rao 2009b; Ifinedo 2014; Vance et al. 2012a). Hence, there is a need to understand other risk management approaches for managing information security risks.

Further, in order to effectively address the "puzzle of information security", there needs to be an understanding of the nature of the perpetrators of the problem – the hackers. Though hacker incidents proliferate the news and popular press, "few rigorously conducted hacker studies have been published, and most of our understanding about computer hackers comes from descriptive accounts and reporting" (Crossler et al. 2013, p. 93). Even though the very nature of their actions presents a difficulty in their accessibility to research, a glimpse of how hackers perpetrate attacks can be obtained through the examination of their knowledge sharing behavior. In general, knowledge is a critical resource that provides a sustainable competitive advantage, and information sharing is a key to understanding that knowledge (Wang and Noe 2010). Hence, gaining some understanding about hackers through their knowledge sharing behavior may help researchers fine-tune future information security research (Crossler et al. 2013). The insights gained from understanding hacker behaviors could also help practitioners design more effective defensive information security strategies, and risk management efforts aimed at protecting information systems resources.

Hence, this dissertation is interested in understanding hackers through their knowledge sharing behavior. Then, of interest also is how individuals form their URL click-through intention in the face of proliferated cyber risks. Finally, we explore how and why top managers who are increasingly accountable for security breaches in their organizations, commit to cyberinsurance as a risk management strategy. Thus, the fundamental research question of this dissertation is**,** "How do individuals and organizations manage information security risks?” To answer this research question, this dissertation investigates three sub-research questions:

(1) Why do hackers share knowledge used in perpetrating cyber-attacks on individuals and organizations? What types of information do they share?

(2) Given a risky Internet environment, what factors shape the individual's decision towards clicking through links on the Internet?

(3) What are the salient factors that determine the top manager’s commitment towards managing information security risk through cyberinsurance?

Three Essays in this Dissertation

Essay 1

The term hacker used to refer to computer programmers that are exceptionally skilled at exploring the boundaries of computer systems. Nowadays, the term has negative connotations and refers to cyber-criminals who break into information systems to compromise and steal information (Young et al. 2007). Today, hackers are known to perpetrate cyber-attacks that result in organizational security breaches which cost the global economy $445 billion annually (Reuters 2014). Hackers continue to wreak havoc on organizations information systems and these hacker incidents proliferate the news and popular press. However, there is a dearth of studies examining their culture and behavior. “Few rigorously conducted hacker studies have been published, and most of our understanding about computer hackers comes from descriptive accounts and reporting” (Crossler et al. 2013, p. 93). Hence, the call for research in hacker communities and behavior (Crossler et al. 2013). In responding to the call, the aim of this essay is to understand the nature of the hacker. The notion is that an understanding of the hacker behavior will provide insights into emerging cyber threats (Benjamin et al. 2016). Further, research that elucidates hacker cybercriminal activities will be beneficial to building information security defenses (Mahmood et al. 2010).

A challenge in examining hacker behavior is that the illegality of their activities render access to this population difficult (Crossler et al. 2013; Young et al. 2007). Even though the very nature of their actions presents a difficulty in their accessibility to research, a glimpse of how hackers perpetrate attacks can be obtained through the examination of their knowledge sharing behavior. Knowledge is a critical resource that provides a sustainable competitive advantage, and knowledge sharing is a key to understanding that knowledge (Wang and Noe 2010). Hence, gaining some understanding about hackers through their knowledge sharing behavior may help researchers fine-tune future information security research (Crossler et al. 2013).

The theoretical lens utilized in this research is social capital theory. Social capital theory (SCT) is a framework for understanding knowledge sharing (Nahapiet and Ghoshal 1998). Scholars of the theory of social capital define social capital as an embedded resources in social networks that can be accessed or used in a purposeful manner (Lin 1999).

Hackers congregate in online forums to share knowledge about hacking tools (Benjamin et al. 2016; Motoyama et al. 2011) and information about their targets (Hausken 2015). Hackers need information, not only about their target organizations or about individuals, but also software, source code, and techniques employed to successfully break into and access their target's information system. Hence, hackers engage in online forums in order to interact with other hackers to exchange knowledge.

Hacker forum archival data is utilized and is accessed from a forum called hackhound.org (Samtani 2016). Using data from 4,242 messages posted by 794 participants in a hacker forum in the US, this study hopes to reveal how hackers approach knowledge sharing and exchange in online networks. Text mining is performed in order to extract topics of interest from forum posts. Content analysis of the posts is performed to explore, understand, and classify the knowledge shared by hackers in the forum. The measures and operationalization of the constructs in this study are based on the literature. To assess knowledge sharing we examined two variables based on the postings: (1) the severity of the shared knowledge to victims and (2) the volume of shared knowledge.

We contribute to research by not only evaluating the hackers' knowledge sharing behavior through the volume of post, but also how the content of the shared knowledge stacks up against known cybercrime attacks. Doing so goes a step further in shedding light on how hacker knowledge sharing behavior is detrimental to individuals and firms (Hausken 2015). Lastly, considering the criminal nature of hacker activities, and the hacker culture that extols the virtues of freely sharing information – "information wants to be free" – this research empirically validates knowledge sharing in the hacker community context. For practitioners, the insights gained could help in the design of more effective defensive information security strategies, and risk management efforts aimed at protecting IS.

Essay 2

The Internet supports different services and functionalities, and has served as a mechanism for the delivery of services, communication and entertainment. Many individuals and organizations now depend on the Internet and applications (Keller, Powell, Horstmann, Predmore, & Crawford, 2005; Knapp & Boulton, 2006) such as search engines for business opportunities and information gathering. As a result, about 88 percent of adults in the US currently use the Internet, and spend more than 20 hours a week on the Internet (GO-Gulf, 2015; Pew Research, 2015). It is no wonder the Internet has become a popular attack vector for malware infections (Financial

Services Rountable, 2011). Attackers often use compromised or legitimately looking fake websites to distribute malware, making it difficult for users to detect (Abbasi et al., 2010). According to a recent vulnerability assessment by Symantec, malware was found on 1 in 566 websites (Symantec, 2014). This supports the prevalence and elevated ranking of malware among the threats to cybersecurity: malware attacks rank highest (Computer Security Institute, 2011). The financial impact of cybercrime is estimated at over $500 billion worldwide each year (Reuters, 2014), and can cause business, personal and social damage (Dinev, 2006). The impact of clicking through a link on the Internet that is malware infected can wreak havoc for the individual, including the stealing of private information (Dinev, 2006) and storing surveillance software on the individuals computer in order to observe their behavior (Grazioli & Jarvenpaa, 2000). Grazioli and Jarvenpaa (2003) argue that deceptions on the Internet threatens the sustainability of e-commerce.

The Internet enables deeper, broader and faster information searches (S. M. Smith & Whitlark, 2001). Attackers exploit search engine sites and e-commerce sites to distribute and spread malware. Given the consequences of clicking on a link that is malware infected, individuals may be discouraged from clicking on legitimate links and completing e-commerce transactions. Thus, endangering e-businesses that depend on click-through to complete online transactions (e.g. e-commerce, search engine results). Hence, in order to retain the Internet as a safe, efficient and effective platform for business transactions, it is important to understand how Internet users form their decisions to click-through URL links in a risky environment. Hence, this study addresses the research question: *"given a risky Internet environment what factors shape the individual's decision towards clicking through links on the Internet?"* Our interest is in understanding why individuals click-through in the presence of the risks involved. We do so using the e-commerce transaction context, while specifically integrating malware risk perception, the risk propensity of using the

Internet and computers, trust, familiarity and self-efficacy of information security as key determinants in online transactions. Using Sitkin and Pablo's (1992) theoretical framework in risky decision making, we show the factors affecting click-through intention. We find that the individual’s intention to click-through is significantly affected by their risk propensity, risk perception, trust of the site, familiarity and self-efficacy of information security.

The individual's interaction with Internet click-through and their perceptions around click-through is under-developed in IS research. Click-through is considered as both a reliable means for showing user preference (Joachims, Granka, Pan, Hembrooke, & Gay, 2005) and a behavioral response (Briggs and Hollis 1997). With respect to a person's decision process, clicks also depict a person's relative preference (Joachims et al., 2005). URL click-through has been used for customer referral, decision judgements, marketing and advertisements (Jansen, Brown, & Resnick, 2007). Click-through represents implicit feedback and indicate relevance judgements and has been used to measure advertising response, and indicate individuals’ immediate interest in a brand (Briggs and Hollis 1997). Thus, this study uses click-through intention to measure the individual's judgement towards a link. If URL links are perceived as unsafe, individuals may not click on them. This represents a huge loss for search engine companies (e.g. Google, Yahoo, and MSN) and e-commerce sites that depend on click-through for revenue (Jansen et al., 2007). Grier, Thomas, Paxson, and Zhang (2010) found that 8% of 25 million URLs posted on Twitter point to malware sites, and suggests that about 0.13% of links on Twitter are clicked on, representing higher URL clicks than clicks from email spam.

Considering the prevalence of cybersecurity threats and the risks of malware on the Internet, studies investigating malware risks on the Internet are sparse. In addition, the coalescing of e-commerce and security research is an important aspect that requires further research. This study applies risky decision making theoretical framework to understand the individual's click-through intention. We also examine the effects of trust and familiarity on the individual’s intention, in the presence of these risks.

This study makes the following contributions to theory and practice. First, it proposes a research model and a set of theory-based hypotheses addressing why individuals click-through and what factors contribute to this behavior. Trust has been used extensively in e-commerce research to explain “how” and “why” individuals engage in e-commerce transactions, but has not been used in understanding risky decision making in the information security context. Second, our study answers the critical question of how trust affects secure behavioral intentions from a cybersecurity standpoint (Pfleeger and Caputo 2012). It does so by integrating trust in the risk framework and by applying the “where” aspects of theory building (Whetten, 1989). The hope is that this research advances information security context-related research, and increases the importance and specificity of trust, risk and security research. In addition, this study provides insights for managerial practices that help enhance click-through of genuine and legitimate links on the Internet.

Essay 3

Security breaches are adversely affecting organizations’ reputation and market value (Cavusoglu et al. 2004; Mukhopadhyay et al. 2013). According to a Forbes report, 46 percent of companies have suffered reputational damage due to a data breach (Forbes 2014). In addition, a recent survey of 2,000 consumers found that nearly 87 percent are unlikely to do business with organizations impacted by data breach (NCI 2016). Ponemon (2015) notes that the average cost of each stolen record is $217. The cost of data breaches include notification of individuals impacted by the breach, legal fees, regulatory fines, and the cost of recovery. These costs can be damaging and difficult to recover from, especially for small and medium sized organizations. These costs are also one of the reasons organizations are driven to protect their businesses from the impact of data breaches by using cyberinsurance. Cyberinsurance as a risk transfer approach is one of the many security risk management strategies used by organizations. Cyberinsurance is an insurance product used to protect organizations from risks derived from the use of the internet and information systems. Cyberinsurance is defined as the transfer of financial risk associated with security/data breaches to a third party (Böhme and Schwartz 2010).

Traditional approaches to security risk management through technology (e.g., Lee and Larsen 2009), policies (e.g., Vance et al. 2012b) and procedures (Spears and Barki 2010) are limited in preventing or eliminating security risks. It is widely understood that identifying and protecting against cyberattacks by technical approaches alone do not provide an overall solution (Majuca et al. 2006; Siegel et al. 2002). Insurance risk management has since focused on reducing the impact and severity of damage through financial means (Siegel et al. 2002). Hence, Majuca et al. (2006) argue that an overall risk management strategy must include cyberinsurance. Cyberinsurance risk management minimizes the impact of financial losses from security and data breaches, allowing organizations to recover quickly from devastating losses and business interruption, thereby contributing to the economic stability of the business environment as a whole.

Consequently, since we know relatively little about how top managers in organizations form estimates of cyberinsurance commitment, this study identifies the determinants and outlines a nomological network that top managers follow in their commitment towards cyberinsurance as a security risk management strategy. Our focus is on the top managers' assessment of the use of cyberinsurance to protect the organizations information assets. There are two reasons this research seeks the top managers perspective. First, organizations consists of individuals that may account for the performance of organizations. Strategic management literature notes that the omission of the individual factors in examining organizations has prevented a thorough understanding of the role individuals actually play in determining firm performance (Mollick 2012). Specifically, it has been shown that top managers are considered to be important in determining firm performance (Bertrand and Schoar 2003; Hambrick et al. 1996; Mollick 2012). The notion is that top managers have a strong influence on how their organizations respond to external and internal events that affect routines, resources and performance (Bertrand and Schoar 2003; Kettinger et al. 2013). In addition, Goodhue and Straub (1991) argue that an organization's protective measures should require managerial careful attention. Second, there is a shifting of accountability in industry, such that top managers - and no longer technology departments - are under increased scrutiny for security breaches (Experian 2015). Top managers are nowadays required to understand and perform recommended actions that prevent and manage the threat of security breaches with cyberinsurance. Hence, this study is interested in understanding the top manager's perspective for the use of cyberinsurance as a risk management strategy. We intend to answer the research question, what are the salient factors that determine the top manager's intention to use cyberinsurance as a risk management strategy?

Using the valence framework of risk and benefits perspective, we identify factors that are inherent in the top manager's commitment towards cyberinsurance. By dimensionalizing the risk and benefit factors along the lines of situational relevant factors and product relevant factors, we seek to extend the valence framework. Situation factors are factors specific to the risks and benefit driving the top manager's commitment towards cyberinsurance. The product factors are specific to the cyberinsurance product. We test the model through a survey of top managers in various organizations. This study seeks to highlight the important role of cyberinsurance as an information security risk management approach. Contributions to research include, theoretically identifying and outlining the factors that determine the top manager’s commitment towards cyberinsurance in a nomological network. For practice, by drawing attention to the relationships between the antecedents and commitment, we hope to spur businesses to consider cyberinsurance as a security risk management strategy.

ESSAY 1

HACKERS DELIGHT: KNOWLEDGE SHARING MOTIVES

1.1 Introduction

Hackers have been identified as primary threats to information systems (IS) and its users (Furnell 2003). They are known to perpetrate cyber-attacks that result in organizational security breaches, which cost the global economy $445 billion annually (Reuters 2014). As hacker exploits continue, researchers (e.g., Abbasi et al. 2014; Crossler et al. 2013; Mahmood et al. 2010) call for more studies examining their culture, characteristics and behaviors. The notion is that an understanding of the nature of hackers will provide insights into emerging cyber threats (Benjamin et al. 2016), and elucidate cybercriminal activities, which are beneficial to building information security defenses (Mahmood et al. 2010). In responding to the call, the goal of this study is to understand the hackers through their knowledge sharing behavior. Even though the very nature of hacker activities present a difficulty in their accessibility to research (Crossler et al. 2013; Mahmood et al. 2010; Young et al. 2007), a glimpse of how hackers perpetrate attacks could be obtained through the examination of their knowledge sharing behavior. Knowledge is a critical resource that provides a sustainable competitive advantage. Knowledge sharing has been described as a key to understanding that knowledge (Wang and Noe 2010). Hence, gaining understanding about hackers through their knowledge sharing behavior may help researchers fine-tune future information security research (Crossler et al. 2013).

While prior studies have contributed to our understanding of traditional knowledge sharing in organizations, we still have much to learn about knowledge sharing within deviant behavior communities. Although knowledge sharing has been studied in online communities (e.g., Faraj and Johnson 2011; Johnson et al. 2015; Wasko and Faraj 2005), the hacker context represents a uniqueness that differentiate it from knowledge sharing in other online communities. First, members of hacker communities are generally known to be hackers who are aware of their illegal activities (Young et al. 2007), and who are seen as threats to information systems (Furnell 2003). Second, the results of the knowledge shared (malware, vulnerabilities, hacking tools, stolen data etc.) can be severe and harmful to individuals and organizations. Hence, it is important to gain a better understanding of the types of knowledge shared in terms of their severity, and the factors that drive sharing of knowledge with different severity. Mahmood et al. (2010) argue that this type of insight will not only help slow the spread and impact of security breaches, but also help in the design of countermeasures that may lessen their damage. By exploring the types of knowledge shared in hacker forums, organizations and security firms may be able uncover advances in security violations, malware distribution, and anti-malware evading techniques. Correspondingly, it is equally important to understand the types of knowledge that are withheld from other hackers, and the conditions for such behaviors. When certain types of knowledge are withheld in the forum, it is possible that it reduces the availability and spread of malicious content.

Knowledge sharing is important in the development of hackers (Jordan and Taylor 1998), and so they congregate to share knowledge (Odabas et al. 2015). In a game theory analysis of knowledge sharing between hackers, Hausken (2015) finds that as the effectiveness of information sharing among hackers increases, information sharing levels and hacker profits increase. Mookerjee et al. (2011) argues that in certain situations, hackers benefit from disseminating security knowledge among one another. In addition, they find that a firm’s cost increases when hackers become more knowledgeable through knowledge sharing within the hacker population. Hence, they conclude that knowledge sharing and dissemination between hackers is damaging to the firm because it increases the firm’s cost.

Even though researchers have identified knowledge sharing in online hacking communities as a key activity for hackers, and that firms' cost increases when hackers share knowledge, there is a gap in the literature investigating why, how, and what types of knowledge hackers share in online hacker communities. A perspective that is also limited is the understanding of the conditions that foster the withholding of knowledge. Hence, we seek to answer the following research questions: *Why do hackers share knowledge in a hacking forum*? *Under what condition will hackers withhold knowledge in a hacking forum*?

Using social network analysis, social capital theory, a framework for understanding knowledge sharing (Nahapiet and Ghoshal 1998), and data from 4,242 messages posted by 794 participants in a hacker forum called hackhound.org, this study explores how hackers approach knowledge sharing, the patterns of knowledge sharing among hackers, and the types of knowledge shared. We also incorporate coopetition literature (e.g., Tsai 2002) to understand withholding behaviors when there is simultaneous cooperation and competition between members of a group. Following recommendations from Wasko and Faraj (2005), this study incorporates additional measures of centrality such as betweenness centrality and boundary spanning using a set of data based on 3 ½ years of sharing in its evaluation of the network structuring. We use an instrumental variable approach to control for endogeneity between the structural variables and dependent variables (e.g. Gu et al. 2012). Furthermore, following Ransbotham and Mitra (2009) that depict hackers attack topology and its severity, we map the content of the knowledge shared in the hacker forum to an existing classification of attack severity.

Our findings suggest that the most influential participants of the online hacker community are those with high degree centrality, betweenness centrality, and boundary span share knowledge in the forum. We also find that individuals with high degree, betweenness, and boundary spanning characteristics withhold sharing knowledge that may be deemed severe in the forum. We contribute to research and practice. First, our main contribution to IS research is in clarifying how forms of social capital facilitates knowledge withholding. By assessing withholding behaviors using forms of social capital, we extend how social capital theory is used in studying knowledge contribution and exchange in IS research. Second, contrary to most research on knowledge sharing in legitimate organizations or online communities, this study contributes to research by providing a finer-grained analysis on how deviant characters such as hackers in an online hacker community interact with each other, and specifically, their knowledge sharing and withholding behaviors. Third, we contribute methodologically to the literature by conceptualizing and categorizing severity of hacking activities, making it possible to conduct quantitative analyses. By quantifying the severity of the shared knowledge, we increase our understanding of the types of knowledge shared by hackers. Lastly, we not only evaluate hackers' knowledge sharing behavior through the volume of post, but also show how the content of the shared knowledge stacks up against existing classification of attack topology (Ransbotham and Mitra 2009). For practitioners, the insights gained could help in the design of more effective defensive strategies and in building adequate risk management capacity.

1.2 Background

Hackers have been described in different ways in the literature (e.g., Décary-Hétu and Dupont 2012; Dupont et al. 2016; Holt et al. 2012; Mookerjee et al. 2011; Thomas 2002). In the 1970s, the concept of hacker was used to describe computer enthusiasts and ardent programmers who explore the limits of computer systems (Thomas 2002). In recent times, the meaning of hacking has evolved to one that denotes hackers and members of hacker communities as threats to information systems and its users (Furnell 2003) and as criminals. Specifically, they are individuals who deliberately gain unauthorized access to systems. Hackers are well aware that their activities are illegal in nature (Young et al. 2007). As argued, an understanding of hackers in online communities must acknowledge the significance of the context that differentiates them from other online communities. Our work builds on few streams of research such as hacker culture, knowledge sharing using social capital theory, and coopetition in explaining the simultaneous collaboration and competition that exists in groups. In the following section, we provide a background of hacker knowledge sharing and the types - in terms of severity - of knowledge shared in the forum.

1.2.1 Hacker Culture and Knowledge Sharing

The hacker culture is driven by the belief that knowledge should be free and that the quest for such knowledge is a human right (Cross 2006). Indeed, studies suggest that the attraction for hackers is the quest for knowledge (Thomas 2005). Even though it makes their illegal activities difficult to hide from law enforcement, knowledge sharing is important in the development of hackers (Jordan and Taylor 1998). Hence, hackers are known to congregate for the purpose of sharing knowledge (Odabas et al. 2015). Given that the primary motivation for hacking is to acquire knowledge (Holt and Kilger 2008; Sarma and Lam 2013), it seems appropriate to gain a good understanding of hackers through an activity that is central to their culture: knowledge sharing behaviors. It has been shown that hacker attacks and knowledge sharing are complements of each of other, such that an increase in one activity leads to an increase in the other (Hausken 2015).

Because hacker community has been seen as heterogeneous (Chantler 1995), a few studies have categorized hackers based on their knowledge transfer capabilities (Zhang et al. 2015). In early hacker days, knowledge sharing was exercised through the physical sharing and exchange of computer tapes and disks upon which the code was recorded (Hippel and Krogh 2003). These days, hackers' knowledge sharing is primarily accomplished through online communities such as online forums and Internet Relay Chat (e.g. Benjamin et al. 2015, 2016). Online communities have been studied in IS specifically to examine why and how individuals share knowledge (e.g., Faraj et al. 2011; Mein Goh et al. 2016). Online communities are known as open collectives of members who are not easily identifiable by others, yet share common interests, the community attends to both the welfare of the collective as well as the individual (Faraj et al. 2011; Sproull and Arriaga 2007). Many online communities have specific focus areas such as social collaborations (Pi et al. 2013), peer-to-peer networks (e.g., Xia et al. 2012), healthcare (e.g., Mein Goh et al. 2016; Yan et al. 2016; Zhang et al. 2017), and open source and innovation (Ho and Rai 2017). Knowledge sharing in traditional online communities involves individuals "offering knowledge to others as well as adding to, recombining, modifying, and integrating knowledge that others have contributed" (Faraj et al. 2011, p. 1). Contrary to traditional online community forums where communication is typically open allowing all members to read all postings (e.g Johnson et al. 2015), the hacker forum posts are not visible to all its members. Different members are allowed access to different subforums and activities based on their social status in the forum. Hence, community members can engage in differentiated knowledge sharing, and have the ability to broker knowledge or span boundaries in the forum increases. In a community that is somewhat closed to the public or that supports exclusive sections, there is usually an opportunity to control information. Thus, it is impossible for all information to be shared with all members of the community (Fleming and Waguespack 2007).

Following previous definitions of knowledge sharing, we define knowledge sharing in hacker context as the provision of task information and know-how about different attack types to help others and to collaborate with others to solve problems and develop new ideas about cyberattacks (Cummings 2004; Wang and Noe 2010). Though Adler and Kwon (2002) argue that the knowledge shared through social relations is tacit rather than explicit in nature, we note that the knowledge shared in this study can be both tacit and explicit. Its tacit nature is due in part to knowledge that may be in bits and pieces making it difficult to transfer to another hacker. It is also explicit because hackers in the forum do share knowledge with each other in the form of source code, programs, or documented formula.

In this study, we theorize how hackers engage in knowledge sharing. Understanding the patterns of hacker knowledge sharing in online communities is important not only because of its prevalent use (open and underground) for training and cultivating more hackers, but also because of the uniqueness of the hacker_context which makes the manner in which they share knowledge important for understanding hackers in general and the types of knowledge they share, specifically. Though similar, the unique difference between knowledge sharing in general online communities and "online offender communities" is that participants in the offender communities are aware of their illegal activities (Young et al. 2007) and also try to protect their anonymity in order to avoid criminal evidence and arrest (Benjamin and Hsinchun Chen 2012). Hackers are known to operate under some disguise and anonymity, where their identities are hidden from others. In most online communities, the type of knowledge shared could be described as helpful to the members and for the society in general. For example, in a health-related forum (e.g., COPD-Support.com, patient.info, and ehealthforum.com) members share diagnosis of diseases, prevention, and knowledge to help each other get better or gain more understanding of their health situation. Whereas, in online hacker communities, the knowledge shared is mostly about vulnerabilities, malware, hacking tools, and stolen data (Holt et al. 2012). Most of which are potentially harmful to individuals, organizations, and the public. As a whole, the elements of anonymity, illegality of activities, coupled with the exchange of potentially damaging knowledge create a degree of uniqueness in knowledge sharing rarely seen in traditional online communities.

1.2.2 Attack Severity and Knowledge Sharing

Severity has been used to understand attack types and assess its risks related to security threats and vulnerabilities (Borges Hink and Goseva-Popstojanova 2016; DeLooze 2004; Symantec 2006). Indeed, security authorities such as Computer Emergency Readiness Team (CERT) and Information Sharing and Analysis Centers (ISACs) are known to use classifications of severity as the basis for determining the urgency and immediacy of information dissemination to its users. Hence, an understanding of the severity of knowledge shared in hacker forums related to attacks may be important to help organizations protect their information assets. In addition, information sharing organizations (ISACs) share cybersecurity threats and attacks information with participating members based on the severity of cyber incidents and attacks (McCarthy et al. 2014). The United States government also follows a classification of severity known as Cyber Incident Severity Schema in its assessment and commination of cyber-attacks (DHS 2016).

Cyber-attack severity has been categorized in many ways including (1) the extent to which malicious programs spread among computer users, (2) the extent of damage a malicious program causes if encountered (Symantec 2006), and (3) the extent that the attack is targeted at a specific system or organization (Ransbotham and Mitra 2009). Using Ransbotham's and Mitra's (2009) approach which is grounded on theory and rigor, we classify attack severity using the extent an attack is targeted at a specific system or organization. Whether an attack is targeted and the extent of targeting is more informative, especially as the attack relates to the motives and identities of the hackers (Kim and Kim 2014). Prior hacker related literature also categorize attacks based on whether they are targeted (e.g. Dey et al. 2012; Png and Wang 2009).

Ransbotham and Mitra (2009) reviewed the literature for attack categories and abstracted the categories into two dimensions in terms of their target specificity and compromise effort. Using these dimensions, Ransbotham and Mitra develops a topology of four attack classifications: *information scans, attack scan, targeted probes, and targeted attacks*. These four attack types are further classified based on their severity, which hinges on their target specificity. Their conceptualization of severity based on whether attacks are targeted or non-targeted lies on two dimensions: high severity and low severity. Although we follow this conceptualization, we scale the degree of severity from (1) not severe to (5) extremely severe. There are a few reasons we do this. First, since computer security community uses 5 severity points (e.g., Symantec 2006) to describe and alert its users of the severity of attacks in an attempt to help victims protect themselves and mitigate the consequential damage (DeLooze 2004), it seems useful to employ similar scale points. Second, it makes it easier to report and communicate findings using such scales to practitioners (Straub and Ang 2008). Third, there is a progression of attacks going from information scans (i.e., information gathering), targeted probes, to target attacks (i.e., system compromise) (Ransbotham and Mitra 2009). Moreover, it has been argued that the extent of targeted attacks is best viewed as degrees of severity rather than dichotomous (Kim and Kim 2014).

Hence, rather than using 0 to 1 (low and high), it seems beneficial to scale these from 1 to 5 to represent a progression of severity.

In order to understand the types of knowledge shared by hackers and classify their severity using the attack types, we performed content analysis of postings in the hacker forum utilizing a text mining method named latent semantic analysis (LSA) (Deerwester et al. 1990). LSA analyzes the textual descriptions of knowledge shared by the hackers. Using the topology of attack severity, a severity score is assigned to extracted topics. The following describes how topics are mapped to attack severity. Tables 1.1 and 1.2 show extracted topics, the attack types, the degree of severity, relevance to knowledge sharing, and example posts. More information on the coding and assignment of topic to severity using Q-Sort is provided in Appendix A.

The topic extraction reveals programming language as a topic in the hacker forum. Hackers share knowledge related to the types of programming languages that newer hackers should learn in order to become proficient. Although learning programming is not an apparent attack, learning through a hacking forum could represent a potential for future attacks. In addition, learning is non-targeted at an organization or information system. Therefore, this topic is designated with a severity degree of 1. *Information scans* refer to the gathering of information about systems. Also referred to as foot-printing,, information scans include the tools and processes to ascertain IP address, open ports, and services running on systems (Ransbotham and Mitra 2009). Information scans are non-targeted and therefore, are low severity attacks. Topics related to tools, processes, and technologies (e.g. IP, proxy, API[1]) for performing information scans are designated with a

[1] An application programming interface (API) is a set of tools (libraries) that allow communications between different software applications. When used for scans, hackers could provoke APIs with ‘unexpected input’ in order to gather information about running services, system capabilities through any error messages, and software version information.

severity degree of 2. The topics depicts problem solving knowledge related to system connectivity, networking, and traffic.

Attack scans are widespread, indiscriminate attempts to damage systems by using malware such as a self-replicating worms (Ransbotham and Mitra 2009) or other types of malware embedded within software programs and documents that are easily downloaded from the internet. The objective of the attack scan is to damage systems. Given that this type of attack is indiscriminate, it is non-targeted at specific systems. Topics related to tools, processes, and technologies for performing attack scans are cracked versions of commercialized software applications and key generators. These tools are used for bypassing licensing and activation mechanisms and for creating product keys of software (Gantz et al. 2006). Crack software are freely available on various websites. Since there is little evidence that hackers are altruistic, the cracked software must fulfil some other purpose. A purpose of cracked software is to exploit program flaws that allow hackers to write Trojan horses, worms, and other malicious code into the software. Attack scans have higher compromise effort than information scans, and are designated a severity degree of 3.

Targeted probes refer to tests of specific information systems for vulnerabilities for the purpose of a later attack. Topics related to tools, processes, and technologies for performing targeted probes are tests for vulnerabilities of specific anti-virus software (e.g. ESET, Kaspersky, Norton). Specifically, hackers test specific antivirus software to ensure the anti-virus bypasses (does not detect) their malware during scan. Topics related to targeted probes are designated with a severity degree of 4.

Table 1.1: Topic Extraction and Example Posts (Essay1)

Topic Extraction	Description	Example Posts
learn, program, language, section, code	Learn programming	"Q: How should I ask programming question when my ***t-code is not working? A: First of all try to understand that you need to learn to walk before you are able to run, so take time to learn your programming language of choice…”
server, IP, problem, proxy, check	Connectivity to server IP, TCP, proxy	“It has nothing to do with the api itself. Comment the function that uses the api, and the detection will be gone.”
crack, version, update, delphi, install	Crack versions and updates	“The 3.8 is cracked, the version i have here is cracked with keygen I work with it, its great...” “Here is the keygen source..nice I’ll [paste] the keygen here”
found, virus, antivirus, security, scan	Antivirus testing	“I checked it and It is clean... No outgoing connections. No injection attempts...” “Yeah…what makes this virus special is that it uses zero-day vulnerabilities…”
source, code, rat, sell	Remote administration tool (RAT)	“Selling source code of bozok rat. It is the newest version (1.6 not released), contains full pe features” “Hey HH members here is another VB.NET sources RAT.. as usual enjoy” “To be honest, I think RAT sources in vb6 are more stable and coded better”

Table 1.2: Classification of Severity of Knowledge Sharing Content (Essay1)

Topic Extraction	Description	Attack Type	Severity Scale	Hacker Knowledge Sharing
learn, program, language, section, code	Learn programming	Foundation	Not severe: 1.	Basic hacking knowledge including general programming is not an apparent attack, but has a potential for future attacks.
server, ip, problem, proxy, check	Connectivity to server IP, TCP, proxy	Information scan	Slightly severe: 2.	Tools, technology and processes for performing information scans.
crack, version, update, delphi, install	Crack versions and updates	Attack scan	Moderately severe: 3.	Cracked version of software and key generators. Hackers use crack software to write Trojan horses into the software.
found, virus, antivirus, security, scan	Antivirus testing	Targeted probe	Very severe: 4.	Targeted probes of specific anti-virus software (e.g., Kaspersky, Norton, ESET). Hackers find vulnerabilities that bypass their malware.
source, code, rat, sell	Remote administration tool (RAT)	Targeted attack	Extremely severe: 5.	Tools, techniques, and processes to compromise targeted systems (e.g. RAT).

Targeted attacks are attempts to compromise specific systems. Topics on tools, processes, and technologies for performing targeted attacks are remote administration tools (RAT). RATs are “system control tools [that] enable the attacker to control sessions and hosts” (Ransbotham and Mitra 2009, p. 128). They are used by cybercriminals to remotely control computer systems (McAfee 2015). Tools such as these are targeted at specific information systems. Targeted attacks are designated with a severity degree of 5.

1.3 Theoretical Foundation

1.3.1 Social Capital Theory

Early review of the social capital literature suggests that social capital is the aggregate of resources held in a network of relationships of “mutual acquaintances or recognition” (Bourdieu 1986, p. 248). Coleman (1988) and Burt (2000) suggest that social capital is the *ability* of actors in a network to gain advantages and obtain benefits as a result of their membership in a social network (Inkpen and Tsang 2005). At an individual level, these benefits include privileged access to hacking knowledge, tools, enhanced understanding of hackers’ norms, and increased reputation. Researchers have noted that access to new sources of knowledge is an important and direct benefit of social capital (Inkpen and Tsang 2005). According to Adler and Kwon (2002, p. 17), social capital is the “*goodwill* that is engendered by the fabric of social relations and that can be mobilized to facilitate action”. Social capital theory has informed our understanding of families, communities, governance, and other collective actions. Scholars have argued that social capital develops in groups that have a shared history, frequency of interaction, and are interdependent on each other (Nahapiet and Ghoshal 1998). In this study, social capital theory is used to understand

and explain how the goodwill, ability, characteristics of the actors (i.e., hackers)[2], and the "function of their location in the structure of the social relations" (Adler and Kwon 2002, p. 18) facilitate patterns knowledge sharing behavior. In particular, we adopt Nahapiet's and Ghoshal's (1998) framework for understanding knowledge sharing through social capital. This framework suggests that knowledge sharing is enabled when (1) individuals are motivated to share knowledge, (2) there are structural ties between the individuals (structural capital), (3) individuals are cognitively capable of applying knowledge (cognitive capital), and (4) they have positive relational characteristics (relational capital). These forms of social capital enable the sharing of knowledge between individuals in a group. Although the framework was based on a group level analysis of knowledge sharing, studies have expounded the importance and relevance of its application in individual level knowledge sharing (Wasko and Faraj 2005).

There are two aspects of knowledge sharing: *cooperative* and *competitive*. The cooperative side of knowledge sharing is the collective use of shared knowledge to pursue common goals. On the other hand, the competitive side refers to the use of shared knowledge to make private gains in an attempt to outperform one's partners (Khanna et al. 1998). According to Khanna et al. (1998), these two sides represent the common benefit and the private benefit. Furthermore, these two sides represent two patterns derived from an early comprehensive review of social capital theory (Adler and Kwon 2002). The first pattern originates from social network theory and suggests that actors derive personal benefits from their social capital (Belliveau et al. 1996; Burt 1997). This pattern views social capital as a private good held by individuals (Inkpen and Tsang 2005). The second pattern views social capital as a public good maintained and enjoyed by a social group. Researchers have argued the need to integrate both aspects of collective and individualist good especially as it

[2] In this study, actors are hackers in hacker communities. We use actors and hackers interchangeably.

relates to knowledge sharing (Krogh 2009) through social capital theory (Inkpen and Tsang 2005). Consequently, definitions of social capital have incorporated both the private and public good perspectives of social capital. In combining both perspectives, previous studies have increased our understanding of knowledge sharing for the public good. For example, after their review of the organizational knowledge sharing literature, Wasko and Faraj (2000) maintains that it is only when knowledge is considered a public good, owned and maintained by a community, will knowledge sharing be motivated by "community interest rather than by narrow self-interest".

However, there is still much to understand about the conditions under which the individualistic or competitive aspects are enacted. That is, what are the conditions for actors to withhold knowledge? By incorporating the hacker culture context in this study, we assess the individualistic or competitive aspects and do so in terms of the type (severity) of knowledge shared. The notion is that individuals through social capital theory, ceteris paribus, will share knowledge in a social network. Conversely, individuals may withhold or not share knowledge depending on the type (severity) of the knowledge. Prior research highlights the importance of context in understanding how social capital factors influence conditions for knowledge sharing (Cohen and Prusak 2001; Nahapiet and Ghoshal 1998). In the next section, we explain the context that allows the competitive aspects of knowledge sharing.

1.3.2 Cooperation

The hackers' online forum is a context where there is simultaneous cooperation and competition among members of the forum. On one hand, the hacker ethos compel them to cooperate and share knowledge. In this case, knowledge sharing is done as a public good. On the other hand, hackers also compete with each other for higher recognition. In this case, individuals perform knowledge sharing activities in order to increase their private benefit, or they may withhold knowledge in order to increase their uniqueness or stock. An environment where there is simultaneous cooperation and competition is referred to as coopetition (Tsai 2002). Coopetition is common in knowledge sharing environments. Given that hackers cooperate and compete, coopetition exists in a hacker community. Coopetition suggests that people will share but also compete to use the knowledge to outperform others, or withhold information. When members of a group compete against one another, knowledge sharing may be reduced (Inkpen and Tsang 2005). Social capital and collective action theories informs our understanding of why and how individuals share knowledge. However, there is little about why and how knowledge is withheld based on public or private good.

In this study, we identity structural capital and cognitive capital as two forms of social capital that affect withholding behaviors. In terms of structural capital, we focus on actor centrality (*degree centrality*, *betweenness centrality*) and boundary span. This understanding can yield insights into how social capital influences private gain in a community. Social network theorists argue that the mechanism for control of knowledge diffusion underlies social capital and draws from actor centrality (Burt, 1992) and boundary spanning (Fleming and Waguespack 2007). In IS literature, these structural capital measures have been used to assess knowledge sharing in social networks (e.g., Johnson et al. 2015; Wasko and Faraj 2005), but not knowledge withholding. It has been argued that factors such as loss of power reduce knowledge sharing behavior and that when individuals share some of their unique knowledge, they relinquish exclusive claim to benefits emanating from such knowledge (Gray 2001; Kankanhalli et al. 2005). Power is inherent in social networks and exists only in relation to others in a network – structural capital (Hanneman and Riddle 2005). In other words, power exists when there are others in the relationship who can be dominated. Degree centrality and betweenness centrality are measures of power in a social network (Hanneman and Riddle 2005). In terms of cognitive capital, we focus on tenure.

Tenure refers to the experience, skill, and expertise possessed by the individual (Wasko and Faraj 2005). The notion is that an individual with a longer tenure, experience, and perhaps more understanding of the impact of severe hacking knowledge is less likely to share higher severity knowledge. Past research suggests that even in the scientific research community, senior researchers tend to withhold knowledge (Haas and Park 2010).

In summary, even though past research argues that loss of power enacted through actor centrality and tenure are barriers to knowledge sharing, we go a step deeper to explore the nature of withholding. First, we suggest that the extent of knowledge withholding is based on the type of knowledge being shared. In other words, when the type of knowledge is general in nature, it can be shared without the fear of losing power. However, when the type of knowledge is more unique or severe, the tendency to withhold (share) increases (reduces). Prior literature tells us that while some types of knowledge can be shared, people are not necessarily willing to share all types of knowledge (Constant et al. 1994). We are also aware that in the hacker community, knowledge that is deemed severe can sometimes be withheld from other members in order to keep that knowledge from "unskilled" hackers (Meyer 1989, p. 44).

Hence, the extent to which an actor shares or withholds knowledge may depend on the type of knowledge shared. Second, even though previous IS research have studied the factors that facilitate knowledge sharing, there is a dearth of research covering knowledge withholding factors through social capital. Therefore, following the theoretical model proposed by Nahapiet and Ghoshal (1998), we develop hypotheses to examine how hacker's characteristics and the forms of social capital (cognitive, relational and structural) relate to knowledge sharing activities. We incorporate simultaneous competitive and cooperative behavior into the knowledge sharing framework, identifying social capital factors that affect withholding behaviors in terms of severity of knowledge.

1.4 Hypotheses Development

1.4.1 Structural Capital

The structural aspect of social capital deals with the pattern of relationships between the individuals in the network. Social capital theory suggests that network connections between individuals predict interaction (Wasko and Faraj 2005). In social networks, it is argued that when individuals regularly interact with each other, the more likely they are to share information. Social networks of relationships play an important role in social, economic, and political interactions and exchanges (Jackson 2008). It has been used to uncover the roles and significance of individuals in a hacker community (e.g., Lu et al. 2010). Structural capital can and is often measured by actor centrality and boundary span in the network. The two most widely used actor centrality metrics are *degree centrality* and *betweenness centrality* (Jackson 2008).

1.4.1.1 Degree Centrality

Social networks are comprised of actors and the relationships between the actors. The actors in this study are the individual hackers engaged in criminal activities in a forum. Actor centrality is used to quantify the importance of actors and indicates that the most prominent actors are strategically located in the social network (Wasserman and Faust 1994). Actors with high degree centrality are known as the experts or leaders in the network. They are the individuals who are “more likely to diffuse new information” (Lu et al. 2010, p. 35). In other words, hackers with high degree of centrality are more likely to share knowledge in the hacker forum.

Another aspect of knowledge sharing related to the type (severity) of knowledge being shared is the evaluation of conditions under which hackers are unwilling to share. For example, knowledge deemed severe can be withheld from other members in order to keep that knowledge from “unskilled” hackers or enforcement agents (Meyer 1989). This is illustrated by a hacker’s account discouraging another hacker from sharing knowledge of a highly severe nature on an online forum:

> …not smart … ‘that computer’ is a system which can be quite powerful if used to its potential. I don't think that information on programming the switches should be released to anyone. Do you realize how destructive [that computer] could really be if used by someone who is irresponsible and intends on destroying things? Don't even think about releasing that file…” (Meyer 1989, p. 44).

Thus, supporting the argument that although some types of knowledge can be shared, people are not necessarily willing to share all types of knowledge (Constant et al. 1994). A hacker with high degree centrality represents a leader with a large proportion of direct ties and in turn, access to a variety of information that can be withheld. Hence, it is possible that hackers with high degree centrality will choose to withhold knowledge with potentially high severity from being available to unskilled hackers.

> H1a: Higher degree centrality is positively associated with more knowledge sharing volume
>
> H1b: Higher degree centrality is negatively associated with higher severity of knowledge sharing

1.4.1.2 Betweenness Centrality

It is the extent to which an actor lies between nodes in a social network, and captures information flows that occur through an individual. *Betweenness centrality* can represent a broker who passes information between actors or a gatekeeper who withholds information from passing between actors in a network. When it comes to knowledge sharing in terms of the volume of knowledge, the tendency to withhold knowledge is less present. Consequently, a hacker with high betweenness centrality is more likely to pass along information to others in the network, and allow knowledge sharing between others. However, the tendency to withhold knowledge can be noticeable when hackers consider the types of knowledge being shared. Indeed, individuals may be unwilling to share all types of knowledge (Constant et al. 1994). This is especially the case in environments where there is both competition and cooperation among the actors, as is the case in hacker communities. Thomas (2005) argues that the growth of online forums created a competition for social status among participants. Although hackers share knowledge in forums in a cooperative style, competition for status and recognition also creates incentives to withhold knowledge from other hackers (Décary-Hétu et al. 2012; Raymond 2000). Coopetition is common in knowledge sharing among competitors (Tsai 2002). Individual will cooperate in knowledge sharing for the collective use of shared knowledge for common interests. Whereas, they compete to use the shared knowledge in order to outperform others (Khanna et al. 1998; Tsai 2002).

Betweenness centrality characterizes actors as having an advantage due to their position between other pairs of actors. The notion is that actors that are between other actors will exercise their power to broker ties between other actors. Hence, other actors will depend on the broker to share knowledge. Betweenness centrality has been described as a measure of communication and knowledge control, and an important network position that is crucial for knowledge sharing in a community (Trier 2008). Individuals with high betweenness centrality are known as brokers and gatekeepers who control the flow of knowledge between sections of the network. This person has control and competitive advantage with respect to access to different types of knowledge and in a position to choose whether to share the knowledge between disconnected actors (Burt 2000). Brokers are characterized as calculating, politically savvy (Burt 1992), and primarily seeking their private gain. Due to the nature of exerting both positive and negative influence, the broker is challenged with balancing the need to simultaneously fill different roles (Fleming and Waguespack 2007; Podolny and Baron 1997). The different roles are the role of diffusing knowledge for the collective benefit and the role of withholding knowledge for private benefit and advancement. Brokers – individuals in a social network that connect disconnected actors – can exploit their network position to advance their private gain. Hence, hackers with high betweenness centrality will not only share knowledge for the collective benefit of others in the forum, but also withhold knowledge with potentially high severity for competitive advantage and private gain.

> H2a: Higher betweenness centrality is positively associated with more knowledge sharing volume
>
> H2b: Higher betweenness centrality is negatively associated with higher severity of knowledge sharing

1.4.1.3 Boundary Span

A simple definition of a group is the distinction between members and non-members, with the group existence depending on the extent to which some individuals are admitted, and others excluded, which allows an observer to create a boundaries around the group (Aldrich and Herker 1977). The boundaries within a hacker forum correspond to interfaces between subforums and threads where each boundary is a demarcation between distinct subforums. Such that admittance to specific subforums are restricted to certain individuals. These boundaries in and of themselves could represent barriers to knowledge diffusion due to the difficulty of sharing different types of knowledge across boundaries (Sorenson et al. 2006). Prior to the Burt’s (1992) classic study on brokering, boundary spanning literature describe boundary spanners as individuals who diffuse knowledge within and across networks (Allen 1977; Tushman 1977). Though measures of betweenness centrality (brokering) and boundary spanning empirically correlate, their concepts are known to differ theoretically. Individuals high in betweenness centrality (brokers) can span boundaries, but not all boundary spanners are brokers (Fleming and Waguespack 2007). In other words, an individual does not need to be a broker in order to control knowledge. A hacker with high boundary spanning qualities is one who can connect knowledge from one thread/subforum to another. Thus, as a function of their role as information processors and external representation (Aldrich and Herker 1977), boundary spanners can diffuse knowledge across multiple subforums. As part of their role in controlling the diffusion of knowledge, the boundary spanner may enact withholding behaviors depending on the type of knowledge. For example, a boundary spanning hacker presented with knowledge that is highly severe in one subforum may choose to withhold and not share that knowledge in another subforum. In contrast to brokers who are more calculating and may withhold for private gains, the literature suggests that the boundary spanners are "guardians who redirect crucial information" (Fleming and Waguespack 2007, p. 166), and may choose to withhold severe knowledge for the collective good.

H3a: Higher boundary spanning is positively associated with more knowledge sharing volume

H3b: Higher boundary spanning is negatively associated with higher severity of knowledge sharing

1.4.2 Hacker Characteristics

Hierarchy in hacker communities is based on knowledge and expertise, where the most senior members are experts or the most technically proficient (Yuwei 2005). Hierarchy is reflected through a hacker's social or expertise status (e.g., expert, intermediate, beginner etc.) in the forum.

Status is defined as an individual's relative position in a social system (Rindova et al. 2006; Stewart and Daniel 2005). Status, in this paper is based on the achievement or experience-oriented status that uses titles such as expert, intermediate etc., to signal competence and superiority. It is not related to the position of situations at particular points in time, as is the case for social media status. Higher status demonstrates prowess and confers many benefits. For example, hackers can use the recognition of a higher social status in one community to join a more established hacking group (Décary-Hétu and Dupont 2013). It is important for hackers to be viewed by other hackers as technically proficient (Andrew Watson). Hence, there is a strong desire to gain a higher social status in the hacker community. In hacker communities, gaining status and recognition is important to hackers (Jordan and Taylor 1998) and the quest for higher status has been known to motivate individuals to participate in knowledge sharing (Hippel and Krogh 2003). A higher status signals that a hacker has demonstrated proficiency.

In addition, social exchange theory suggests that individuals interact with others based on their expectation of social rewards such as recognition, status, and respect (Wasko and Faraj 2005). The hacker culture has been described as a gift culture, where status is gained by giving away source code, participating in testing other hacker’s source code, and growing the group through questions and answers (Raymond 2001). Forum administrators are known to assign status to individuals based on their contributions (volume), as well as the quality and type of knowledge shared. Administrators could also downgrade or upgrade individuals’ status, which also acts as a behavioral control mechanism (Monsma et al. 2013). Hence, a hacker may share knowledge deemed more severe in its consequences in order to garner higher status. This is further illustrated by a hacker’s account: “a good hack is a bigger thrill when shared and can contribute to a hacker gaining status and access to more communal expertise” (Jordan and Taylor 1998, p. 764). Previous research found that individual motivations such as reputation and status affect knowledge sharing (Wasko and Faraj 2005; Yan et al. 2016). Based on these arguments, we expect that higher status hackers will have more knowledge sharing posts and share knowledge with higher severity.

H3a: Higher status is positively associated with more knowledge sharing volume

H3b: Higher status is positively associated with higher severity of the knowledge sharing

1.4.3 Cognitive Capital

Previous studies have found that cognitive capital – measured as tenure – predicts knowledge sharing and contribution in a social network (e.g., Wasko and Faraj 2005). Cognitive capital consists of the individual’s expertise, their experience with using the expertise, and their mastery of the application of that expertise (Wasko and Faraj 2005). Wasko and Faraj (2005) argue that an individual’s cognitive capital increases over time as they interact with others and share knowledge and norms of the group in which they belong. They further argue that tenure in a shared practice serves as a measure of cognitive capital. In a hacker forum, even when a hacker is motivated to share knowledge, sharing is unlikely unless the hacker has the necessary cognitive capital. For example, a hacker who does not have expertise in malware re-engineering targeted at a specific software would not be able to share knowledge related in that subject matter irrespective of his/her structural capital, motivation, or relational capital. Hackers with longer tenure in the hacker forum are more likely to better understand how to apply their expertise and the relevancy of their expertise. Therefore, hackers with longer tenure are better able to share knowledge with others. Tenure in a hacker community impacts interaction with other members because tenure generally amplifies an individual’s expertise (Benjamin and Hsinchun Chen 2012).

In addition, hackers with longer tenure and more experience understand the impact of higher severity knowledge. Hence, it is possible that a member who has longer tenure, experience, and perhaps more understanding of the impact of severe hacking knowledge is less likely to share higher severity knowledge; more especially when this type of knowledge is shared with the general hacker population in the forum. The same rationale may hold when senior level personnel, for example, knowingly withhold sensitive information from junior officers over concerns of leaks or of fear of inappropriate use. Even in the scientific community where sharing of knowledge is seemingly the norm – for the advancement of science – it is often common for the more senior researchers to withhold information from others. Hass and Park (2010) in their research regarding withholding in the scientific community describe such withholding tendency as - "*The PI [principal investigator] was afraid I'd maybe say something I shouldn't [about details of the technology that might enable others to replicate it]. He asked to review the slides. He said, "Don't talk too much about this—don't give too much detail*" (2010, p. 878). Hence, we posit that higher tenured hackers not only share more knowledge in the forum, they also withhold sharing higher severity knowledge.

H4a: Longer tenure is positively associated with more knowledge sharing volume

H4b: Longer tenure is negatively associated with higher severity of knowledge sharing

1.4.4 Relational Capital

Knowledge sharing in a network also results from the affective nature of relationships within a collective (Nahapiet and Ghoshal 1998). This affective aspect, called relational capital exists when individuals trust others, develop an identity with the collective (Wasko and Faraj 2005), or adhere to the norms of the group (Putnam 1995). We focus on the relational capital of norms of hacker communities. A norm has been described as the extent to which consensus is held in a social system (Coleman 1990; Nahapiet and Ghoshal 1998). We view norms as regulated expectations (e.g., a rule) for members of a group (Haas and Park 2010). Norms of sharing create, transform, and invoke shared interest and a commitment of a common goal. Without shared norms of behavior, sharing knowledge would be challenging (Coleman 1988). Norms require maintenance and periodic renewal in order for it to retain efficacy (Adler and Kwon 2002). In addition, the effectiveness of norms is often maintained through sanctions. Put together, for norms to be effective, there needs to be periodic exposure to the norms and a sanctioning mechanism for non-adherence. Effective norms in hacker communities require its members to share knowledge. The influence of exposure of written norms on behavior has been studied in previous research (Campo and Cameron 2006; Perkins and Craig 2006). Such exposure include print messages and emails that encourage certain behaviors.

The theory of planned behavior (Ajzen and Fishbein 1977) suggests that subjective norms influence behavioral intentions. For example, studies found that norms have a significant effect on knowledge sharing intentions (Hau and Kim 2011). Most communities share norms that guide what constitutes acceptable behaviors and activities. The same is true in hacker communities where members are exposed to written norms (i.e., written rules) that encourage members' posting. Members of the hacker forum share membership norms to help new hackers learn appropriate behavior, and help older members teach beginners (Raymond 2000). For example, a hacker's exposure to norms of behavior in the hacker forum inform members about how many posts are required in order to advance in status or utilize other forum functions. The most common written rules appearing on posts are "please login or register to see this hidden content, you cannot view this content", for which a member asks, "Why does it say [you] can not view the hidden content?" Another member responds, "You need more posts. Minimal amount needed to view urls and other content is 2." From this account, we see both the exposure to norms and the sanctioning mechanism that limits the type of content one can access when norms are not followed.

Norms can also encourage posts that have higher severity. An example of written norms that may affect severity of posts is in this account, “[I] tried to pm[3] you but [I] need at least 5 posts... I can't pm you and don't want to spam few topics just to bypass the forum rules….Which crypters work with netwire?” In this example, the member acknowledges the norm, abides by the norm (i.e., posting of relevant rather than spam topics), and at the same time initiates a post that is potentially severe (e.g., crypters, netwire). Netwire is a remote RAT used by cybercriminals to remotely control computer systems (McAfee 2015). When other members respond to the question about ‘netwire’, they abide by the norm of posting relevant knowledge while at the same time posting knowledge with higher severity. Because forum norms capture the written rules of expected behavior, we argue that increased exposure to the norms will increase knowledge sharing in the forum and increase sharing of knowledge with higher severity.

H5a: Increased exposure to hacking forum norms is positively associated with more knowledge sharing

H5b: Increased exposure to hacking forum norms is positively associated with higher severity of knowledge sharing

1.5 Research Methodology

1.5.1 Data

In this study, we use a set of secondary archival data from a hacker forum accessed from hackhound.org (Samtani 2016). We obtained multiyear archival data with 4,242 messages posted by 794 community members in a hacker forum in the United States. Participation in hackhound.org is anonymous. The forum only allowed browsing of some information without registration. However, full participation requires users to register with the forum using a pseudonym. Since all

[3] PM means private message

members of the hacker forum share similar interests, we refer to members of the forum as hackers (Zhang et al. 2015). The data includes messages, message postdate, threads, user status, pseudonyms, and user start date in the forum. The data is from October 2012 to September 2015. Table 1.3 summarizes the descriptive statistics of the archival data. Table 1.4 depicts the frequency of knowledge severity, which shows that knowledge related to RATs garnered the most posts (30%). It also shows that 57% of discussions in the forum center on antivirus software testing for malware evasion and malicious remote administration tools.

Table 1.3: Hacker Forum Descriptive Statistics (Essay1)

Hacker Forum	Statistics
Number of hackers	794
Number of messages	4,242
Number of Threads	697
Average tenure (Number of weeks in forum)	513
Span of posts (in days)	1074 periods

Table 1.4: Severity of Knowledge Frequency (Essay1)

Severity	Knowledge	Frequency	Percent
1	Learning	850	26.0
2	Connectivity, server, API, IP, proxy	418	12.8
3	Crack versions and updates	129	4.0
4	Antivirus testing	874	26.8
5	Remote administration tool (RAT)	993	30.4
Total		3264	100.0

1.5.2 Variables

1.5.2.1 Dependent Variables

We measure knowledge sharing using two variables: (1) the total number of posts by each hacker – *PostCount*, and (2) the severity of the knowledge posted – *PostSeverity*. For PostSeverity, we performed content analysis using text-mining techniques to extract topics from the message posts. The extracted topics are then mapped using attack topology – information scans, attack scans, targeted probes, and targeted attacks. Then, the extracted topics are coded based on whether the knowledge share related to Ransbotham and Mitra's (2009) attack topology is severe on a scale of not at all severe (1) to extremely severe (5). (See Appendix A). The text-mining tool also provides a text (post) to topic association. In other words, it maps each hacker's post to an extracted topic. Since each topic has been given a severity score, it follows that each hacker's post is mapped to a topic's severity. Severity is rated and scored for each post using the mapping from Table 1.2.

1.5.2.2 Independent Variables

Status is derived from the member's hierarchical status in the forum. Status usually consists of multiple status groups (e.g., expert, intermediate, newbie, beginner, banned). Hence, it is conceptualized as items on an ordinal scale (Bitektine 2011). Members may hold 2 – 3 different titles during their tenure in the forum. For example, a user might have had a status of 'beginner' at the start of their membership to the forum. Further posts by this same user will also have 'expert' or 'member' as their status, indicating that their status changes as their activities evolve in the forum. The status titles are coded based on expertise on a scale of 1 – 4, where 4 is the highest status and 1 is the lowest. The following are guidelines for coding the status. Advanced member, advanced, and expert titles are coded as 4. Hackers coded with this status scale act as moderators of the forum and represents how much experience the user has in the forum. Intermediate member, intermediate and member titles are coded as 3. Hackers coded with this status scale have been verified and upgraded from beginner or newbie status, have provided valued knowledge to other members. For example, when a member receives a 'verified' status from a moderator, it is indicative of the members credibility (Radianti 2010). Newbie and beginner titles are coded as 2. Hackers coded with this status scale are new users in the forum and are yet to be verified. Banned, suspended, retarded and Ub3noob[4] are coded as 1. Hackers coded with this status have either had some unresolved conflict with other members or failed to follow the norms and rules of the forum. The banned status signifies a hacker who is no longer allowed to participate (Radianti 2010).

Degree centrality and betweenness centrality are calculated using R program and UCINET 6 program (Borgatti et al. 2002) for the analysis of social network data. *Degree centrality* can be separately calculated and analyzed as in-degree and out-degree. In-degree is the number of ties received and the out-degree is the number of ties initiated by an actor. Our calculation consists of both in and out degree, which means the data consist of the sums of the values of the ties (in and out). *Boundary span* is measured as the ratio of the number of unique message threads posted, divided by total number of posts (Johnson et al. 2015). *Tenure* in the forum is a proxy for experience. Following Wasko and Faraj (2005), hackers tenure is used as a measure of cognitive capital and is measured by the number of days in the hacker forum (Benjamin and Hsinchun Chen 2012). *Norm* is a shared consensus held in the forum and is measured by the frequency of a hacker's exposure to the written rules that guide acceptable behaviors. It is a count of the total

[4] Individuals who are inexperienced and yet not interested in learning. It is often used as an insult. Many variations include n00b, noob (Calka 2006).

number of times that written rules (e.g., you cannot view this content, please login or register to see this hidden content) are displayed on a member's post.

Table 1.5 summarizes the definition of each variable and Table 1.6 provides the summary statistics of the pooled data, depicting the *within* and *between* variations of the variables. In terms of betweenness, there are large variations (1488.72) over time for individual hackers and a large variation across individuals (319.21). Given that the within variation is larger than the between variation, this indicates that hacker's brokering characteristics vary throughout. Similarly, the within (135.69) and between (46.42) variations in *degree centrality* are pronounced but less so than *betweenness centrality*. The structural capital of boundary span shows no variation over time for individual hackers (0) and very little variation across individuals (.24). Another variation that can be noticed is tenure, which has a large variation across individuals (285.62).

Table 1.5: Variable Definitions (Essay1)

Variable	Type	Description
PostCount	Count	Volume of posts of each member
PostSeverity	Scale	Severity of the knowledge posted derived from the message content and scaled from not severe (1) to extremely severe (5)
Degree	Structural	Degree centrality of a member
Betweenness	Structural	Betweenness centrality of a member
Boundary spanning	Structural	Ratio of number of unique message threads posted divided by total number of posts
Tenure	Cognitive	A proxy for experience
Norms	Relational	Frequency of a hacker's exposure to the written rules that guide acceptable behaviors
Status	Individual	Member's hierarchical status in the forum (e.g. beginner, member etc.)

Table 1.6: Summary Statistics of Within and Between Variations of Key Variables (Essay1

Variable		Mean	Std. Dev.	Min	Max
PostCount	overall	104.45	164.38	1	490
	between		23.02	1	490
	within		0	104.45	104.45
PostSeverity	overall	2.08	.98	0	5
	between		1.60	0	5
	within		0	2.08	2.08
Betweenness	overall	1286.71	2480.50	0	10765.84
	between		319.210	0	5952.22
	within		1488.72	-4515.19	6100.33
Degree	overall	182.22	254.65	0	1147
	between		46.42	0	680.29
	within		135.69	-407.07	648.92
BoundarySpan	overall	.62	.21	.13	1
	between		.24	.13	1
	within		0	.62	.62
Norm	overall	4.66	9.05	0	29
	between		1.38	0	29
	within		0	4.66	4.66
Status	overall	2.75	1.08	0	4
	between		.84	0	4
	within		.20	-.95*	3.68
Tenure	overall	700.18	289.94	1	1073
	between		285.62	1	1073
	within		0	700.18	700.18

Note: Observations (N) = 4,236, participants (n) = 794

1.6 Model and Data Analysis

Using Stata 14.2, we regress both *PostCount* and *PostSeverity* on correlates of degree centrality, betweenness centrality, boundary span, norm, status, and tenure. Even though it is possible that the independent variables used in this study are endogenous, we mainly rely on theory to model the variables (e.g., degree and betweenness centrality) as independent variables, and *PostCount* and *PostSeverity* as the dependent variables. Social capital theory suggests that social structure (e.g. degree centrality and betweenness centrality) facilitates actions taken by individuals within a structure or network (Coleman 1988, 1990; Nahapiet and Ghoshal 1998). In addition, previous studies using social capital theory have confirmed the relationships between structural capital and knowledge sharing. For example, Wasko and Faraj (2005) found that degree centrality is positively associated with knowledge contribution. Other studies also note that knowledge transfer and sharing are facilitated by network positions and social interactions (Inkpen and Tsang 2005; Yli-Renko et al. 2001). Nevertheless, to alleviate possible bias concerns we use multiple models. First, we use ordinary least squares (OLS) model. Then, we use an instrumental variable approach to address potential endogeneity biases.

Corrections are made for potential autocorrelation and heteroscedasticity in the data. To correct for heteroscedasticity, we use White standard errors (White 1980). To control for autocorrelation, we use Newey-West autocorrelation and heteroscedasticity consistent estimators (Newey and West 1987). Furthermore, we formally assess multicollinearity by examining the variance inflation factor (VIF) statistics and find that degree and betweenness centrality are both above 10, which is the rule of thumb for multicollinearity (Kennedy 2003). To overcome multicollinearity issues, we calculate centrality measures per six months (e.g. Yaraghi et al. 2015). This not only brought the VIFs below 10, it also increased the dynamic nature of the variables.

The highest VIF values for the independent variables is 3.24. The VIF values are shown in Tables 1.7, 1.8, 1.9, and 1.10. Table 1.7 shows the correlation matrix of the independent variables. The correlations among the variables are significant. Though some of the measures are highly correlated, we note that social capital measures tend to be highly related (Nahapiet and Ghoshal 1998).

Table 1.7: Correlation of Key Variables (Essay1)

	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**
(1) Betweenness	1					
(2) Degree	-0.4388	1				
(3) Norm	-0.3172	0.4098	1			
(4) Status	-0.0265	-0.3035	-0.2590	1		
(5) Tenure	0.0789	-0.0705	-0.6170	-0.3882	1	
(6) BoundarySpan	-0.2400	0.3452	-0.0348	-0.0519	-0.0610	1

1.6.1 Regression Model

We first estimate the following ordinary least squares (OLS) regression model. The models for *PostCount* and *PostSeverity* are similar except for the dependent variable names. Formally, we estimate the following model:

$$\begin{aligned} &PostCount_{it} \\ &\quad = \beta_0 + \beta_1.\, Degree_{it} + \beta_2.Betweenness_{it} + \beta_3.Norm_{it} + \beta_4.Status_{it} \\ &\quad + \beta_5.Tenure_{it} + \beta_6.BoundarySpan_{it} + \varepsilon_{it} \qquad (M1) \end{aligned}$$

$$\begin{aligned} &PostSeverity_{it} \\ &\quad = \beta_0 + \beta_1.\, Degree_{it} + \beta_2.Betweenness_{it} + \beta_3.Norm_{it} + \beta_4.Status_{it} \end{aligned}$$

$$+ \beta_5.Tenure_{it} + \beta_6.BoundarySpan_{it} + \varepsilon_{it} \qquad (M2)$$

The OLS results for *PostCount* and *PostSeverity* are summarized in Tables 1.8 and 1.9, respectively. The OLS estimator uses both between and within variation to estimate the parameters. Similar to results found by Gu et al. (2012), we also find that the estimation results for White and Newey-West are qualitatively similar. Hence, we report only White's estimation results. Appendix B shows both White and Newey-West results. The results show that *PostCount* and *PostSeverity* are significantly affected by degree centrality and betweenness centrality, thus, H1a, H1b, H2a, and H2b are supported. Boundary span is also significant in its relationships with *PostCount* and *PostSeverity*. Hence, H3a and H3b are supported. Status is significant in its relationship with PostCount; however, it is not significant with PostSeverity. Thus, H4a is supported whereas H4b is not. Tenure positively affects *PostCount* and negatively affects *PostSeverity*, supporting H5a and H5b. In addition, norm positively affects *PostCount* and *PostSeverity*. Thus, H6a and H6b are supported.

Table 1.8: Result of the OLS estimation for PostCount of M1 (Essay1)

Independent Variables	**Estimate**	**Std. Err.**	**t value**	**P>|t|**	**VIF**
Betweenness	0.0024692	0.00052	4.75	0.000	3.24
Degree	0.2028047	0.0027029	75.03	0.000	2.43
Norm	11.50776	0.1523463	75.54	0.000	2.33
Status	13.46421	0.7669202	17.56	0.000	1.53
Tenure	0.0359135	0.0019154	18.75	0.000	1.40
BoundarySpan	7.544179	2.452652	3.08	0.002	1.12
Observations: 4,236; Sample: 794; R-square: 0. 9146					

Table 1.9: Results of the OLS estimation for PostSeverity of M2 (Essay1

Independent Variables	Estimate	Std. Err.	t value	P > |t|	VIF
Betweenness	-0.0000057	0.0000020	-2.87	0.004	3.24
Degree	-0.0002107	0.0000323	-6.52	0.000	2.43
Norm	0.0044392	0.0010086	4.40	0.000	2.33
Status	0.0159207	0.0177701	0.90	0.370	1.53
Tenure	-0.0004434	0.0000723	-6.13	0.000	1.40
BoundarySpan	-0.6473392	0.0942528	-6.87	0.000	1.12
Observations: 4,236; Sample: 794; R-square: 0. 0323					

1.6.2 2SLS - Instrumental Variables

Although the theoretical relationships in our model are established based on social capital theory (e.g. Burt 2000; Nahapiet and Ghoshal 1998; Wasko and Faraj 2005), we ensure the robustness of the model by accounting for endogeneity using the two stage least squares (2SLS) method, which implements instrumental variable estimation. To control any possible endogeneity between degree centrality and PostCount and PostSeverity, we conduct an instrumental variables (IV) analysis using *ThreadStarted* and *ThreadCount* (e.g. Gu et al. 2012). The rational for using these variables as instruments is as follows. In the hacker forum that we studied in this paper, *ThreadStarted* refers to whether a hacker ever started a thread (i.e. conversation). *ThreadCount* refers to how many threads a hacker started in the forum. The default behavior in a forum is to follow a conversation that is already started and post messages in response in the thread. However, starting a new thread where a hacker creates a new topic and controls the conversation can increase the degree centrality of the individual. Values of 1 and 0 signify a yes and no for *ThreadStarted*, while *ThreadCount* is the total number of threads started. The instrument variables meet three requirements. First, they are correlated with degree centrality (see Appendix C). Second, they are uncorrelated with the error term, meaning that they are not endogenous. Third, they are not a direct cause of the dependent variables (PostCount, PostSeverity). Since their relationships to the dependent variables and aspects of their characteristics are similar (Fleming and Waguespack 2007; Johnson et al. 2015) in our model, we estimate using only boundary span, rather than boundary span and betweenness centrality. Formally, we estimate the following models for PostCount and Post severity:

$$\begin{aligned} PostCount_{it} &= \beta_0 + \beta_1.Degree_{it} + \beta_2.BoundarySpan_{it} \\ &+ \beta_3.Norm_{it} + \beta_4.Status_{it} + \beta_5.Tenure_{it} + \varepsilon_{it} \qquad (M3) \end{aligned}$$

$$\begin{aligned} PostSeverity_{it} &= \beta_0 + \beta_1.Degree_{it} + \beta_2.BoundarySpan_{it} \\ &+ \beta_3.Norm_{it} + \beta_4.Status_{it} + \beta_5.Tenure_{it} + \varepsilon_{it} \qquad (M4) \end{aligned}$$

We formally test for endogeneity relying on Hausman (1978), which compares OLS and 2SLS estimators. For the *PostCount* model, we identify and use only the *ThreadStarted* instrument. The null hypothesis that the degree centrality is exogenous, is not rejected. We do not find evidence of endogeneity of (Du-Wu-Hausman F (1, 4228) = .0196; *p* = 0.8885). We also test for weak instruments, which relies on F statistics for an estimate of the joint significance of the instruments used. The F statistics of 295 is larger than 10, which is the rule of thumb threshold for weak instrument (Staiger and Stock 1997). Therefore, the instrument is not weak. For the PostSeverity model, we only use the *ThreadCount* instrument. When we test for endogeneity, we fail to reject the hypothesis that degree centrality is exogenous (Du-Wu-Hausman F (1, 4228) = .23876; *p* = 0.6251). The weak instruments test results in an F statistics of 137. Tables 1.10 and 1.11 report the results of the 2SLS estimation. The result of the 2SLS estimation supports the OLS results. Furthermore, we acknowledge that the R-square is low but has been deemed acceptable for such data (Hinz and Spann 2008).

Table 1.10: Result of the 2SLS Estimation for PostCount of M (3)

Independent Variables	**Estimate**	**Std. Err.**	**z**	**P>|z|**	**VIF**
Degree	0.2218746	0.0215576	10.29	0.000	1.60
Norm	0.0351525	0.002478	14.19	0.000	1.66
Status	13.15918	1.362766	9.66	0.000	1.53
Tenure	11.74429	0.2492913	47.11	0.000	1.40
BoundarySpan	10.34322	4.4646	2.32	0.021	1.11
Observations: 4,236; Sample: 794; R-square: 0. 9142					

Table 1.11: Result of the 2SLS Estimation for PostSeverity of M (4)

Independent Variables	**Estimate**	**Std. Err.**	**z value**	**P>|z|**	**VIF**
Degree	-0.0003804	0.0001784	-2.13	0.033	1.60
Norm	-0.0004326	0.0000708	-6.11	0.000	1.66
Status	0.023356	0.0214893	1.09	0.277	1.53
Tenure	0.0051806	0.002046	2.53	0.011	1.40
BoundarySpan	-0.6723746	0.1030009	-6.53	0.000	1.11
Observations: 4,236; Sample: 794; R-square: 0. 0313					

1.6.3 Robustness Checks

We performed robustness checks to ensure confidence in our results. First, we performed an OLS estimation model, and then we ran a 2SLS model and got similar results. Also, after comparing estimates and standard errors corrected for heteroscedasticity and autocorrelation using White (1980) and Newey-West (1987), we use White's (see Appendix C). Overall, the robustness checks suggest that the findings from our data analyses are robust and hold well using different models and estimators.

1.7 Discussion

As hackers' exploits continue to threaten information systems (Furnell 2003), researchers call for studies examining their behaviors (Abbasi et al. 2014; Crossler et al. 2013; Mahmood et al. 2010) in hopes that an understanding of their behavior will provide insights into emerging cyber threats (Benjamin et al. 2016).. In responding to the call, we seek to better understand hacker behavior by examining why they share knowledge, the types of knowledge shared, the patterns of knowledge sharing among hackers, and the condition under which knowledge is withheld from others.

In terms of knowledge sharing volume, our findings suggest that *degree centrality* and *betweenness centrality* of hackers lead to increased knowledge sharing. Thus, the links between members of the forum spur interactions. This supports knowledge sharing literature that suggests structural ties lead to knowledge sharing (e.g. Wasko and Faraj 2005). *Boundary spanning*, another form of structural ties, is also found to increase knowledge sharing volume. This supports the literature in online social networks (e.g. Johnson et al. 2015) that suggest that because boundary spanners are present in multiple threads or conversations in the forum, they tend to share more knowledge. In addition, we find that norms, status, and tenure lead to increased knowledge sharing volume.

In terms of knowledge sharing severity, our results support our hypotheses. *Degree centrality* and *betweenness centrality* are significantly negative in their relationship with knowledge sharing severity. In addition, boundary span is also negative in its relationship with knowledge sharing severity. Degree centrality suggests that well-connected leaders in the forum might not share knowledge deemed severe in the forum. The result of the relationship between *betweenness centrality* and severe knowledge also suggests that actors in between nodes in a social network will enact their gatekeeper role by withholding knowledge deemed severe from passing through. The same is true for boundary spanners who engage in multiple conversations, they may also withhold knowledge from passing from one thread to another. We also found a negative relationship between tenure and knowledge sharing severity. This suggests that hackers who have stayed in the forum for a longer time and perhaps understand the impact of severe knowledge, may not be inclined to readily share that type of knowledge. Lastly, knowledge sharing severity is affected positively by status and norms. A hacker forum is an expertise-based environment where social status is gained based on one's display of expertise. Given that hackers always seek recognition and status (Décary-Hétu et al. 2012; Raymond 2000), these relationships suggest that hackers have a tendency to share knowledge that is severe in nature in order to demonstrate their expertise.

1.7.1 Research Implications

This study makes several unique contributions to the understanding of hacker behaviors through social capital theory. First, contrary to most research on knowledge sharing in legitimate organizations or online communities, this study contributes to research by providing a finer-grained analysis of how deviant characters of hackers in an online hacker community interact with each other, and specifically, their knowledge sharing and withholding behaviors. Beyond the types of knowledge hackers share in the hacker communities, we also gain some understanding of the types of knowledge they withhold from others. From a theoretical perspective, this provides a balanced viewpoint of knowledge sharing in hacker communities. Second, our findings lend support to the oft-proposed (e.g. Burt 2000) but hardly explored link between structural ties and knowledge control. By extracting structural capital measures (degree centrality, betweenness centrality, and boundary span) and incorporating them as variables in our model, we are able to assess the relationships between these measures and knowledge sharing and withholding behaviors. In so doing, we offer a deeper understanding of knowledge withholding behaviors. For example, we are able to show the likelihood that leaders (degree), well-connected gatekeepers (betweenness), and senior hackers (tenure), will withhold highly severe hacking knowledge in a forum. Third, by assessing withholding behaviors using forms of social capital, we extend how social capital theory is used in studying knowledge contribution and exchange in IS research. Methodologically, this also provides an avenue for assessing knowledge sharing and withholding behaviors in other network structures in general. For example, the method used in this study can be applied in other areas to identify how and why leaders or connected members share or withhold knowledge in online communities. Fourth, we contribute to the literature by conceptualizing and categorizing severity of hacking activities, making it possible to conduct quantitative analyses. By elucidating the methods used in the research, we show the effectiveness of using text mining and social network analysis. Using similar tools, security researchers could continuously identify the content of interest to hackers, and benefit from gaining more understanding of the hacker culture.

Perhaps, this will help researchers identify real threats and provide insights to how they can be addressed. Lastly, by using existing classification of attack topology and severity, we contribute to research by not only evaluating the hackers' information sharing behavior through the volume of post, but also how the content of the shared knowledge stacks up against known cyber-attacks.

In conclusion, our main contribution to IS research is in clarifying how forms of social capital can lead to knowledge withholding. We found reasonable empirical support for the possibility of certain social capital effects explaining the distinctive nature of knowledge sharing and withholding behaviors.

1.7.2 Managerial Implications

Our results can inform information security managers regarding whether knowledge with high severity is shared in hacker forums. First, our findings provide a glimpse of the positive externalities of patterns of behavior that may have an overall benefit to individuals and organizations. For example, the results show that higher tenure and highly connected individuals tend to withhold highly severe knowledge. Although this behavior may be due to private good competitiveness, it nonetheless results in the reduction of severe knowledge in the general forum where nonskilled hackers - who do not fully understand its impact – can access. Second, the literature on knowledge sharing tells us that new discoveries and innovation emerge when individuals share and contribute knowledge in a group (Krogh 2009). By exploring the types of knowledge shared in the hacker forums, organizations and security firms might be able uncover innovations in security violations, trends in malware distribution, and anti-malware evading techniques. For example, Table 1.4 shows that 57% of discussions in the forum center on antivirus software testing for malware evasion and remote administration tools. Thus, the indication that hackers in the forum are interested in these topics may spur or increase risk management capacity for security software vendors and security managers.

Furthermore, the interest in RATs in the hacker forum should also inform security managers' focus on specific security awareness training for users and detection software geared towards identifying and removing RAT software. Third, social capital is located in the relationships that actors share with others, rather than in the actors themselves. When an actor is removed from the network of relationships, the social capital that exists in the relationships held by that actor disappears. By using social capital theory and network analysis in this study of hackers' forum, we identify hackers with the most social (structural) capital. Methodologically, this process could potentially be used to identify bad actors in criminal networks. The withdrawal of such actors (by law enforcement) may serve to dissolve the social capital they wield.

1.7.3 Limitations and Future Directions

This study has some limitations that create multiple opportunities for future research. First, since this is the first study in IS to empirically explore the relationship between structural capital, cognitive capital, and knowledge withholding behaviors, more research is needed to validate the effects. In addition, more research is warranted to identity other social capital measures associated with withholding behaviors. This study validates that social capital measures usually assessed in legitimate organizations also work in the deviant character communities such as a hacker forum – as far as knowledge sharing volume is concerned. Hence, it is quite possible that the factors affecting withholding behaviors in hacker forum may also hold in certain communities and under specific conditions where knowledge may be sensitive, private with severe consequences if exposed, confidential, or tagged with specific classifications. Second, although this research contributes to our understanding of hacker behavior and provides an exploratory starting point for understanding the hacker knowledge sharing behaviors, it is possible that the hacker forum used in this study is not representative of all hacker forums. Hence, incorporating more hacker forums in the data analysis may improve generalizability of the findings. Lastly, as is the case with archival data this research is limited to the available variables that can be assessed for a better understanding of the phenomena. On the other hand, using archival data perhaps gives this research higher generalizability due to the fact that it does not suffer from perception based survey methods.

1.8 Conclusion

In responding to the call to better understand hacker behavior, this study uses social capital theory, social network analysis, and data from hacker forum participants over a 3-year period to explore how hackers approach knowledge sharing and withholding behaviors. To investigate how social capital factors lead to withholding of knowledge, first, we map the content of the knowledge shared in the hackers forum with existing classification of attack severity. Then, we regress social capital factors on knowledge sharing severity. Our findings indicate that hackers share knowledge, but will withhold some knowledge based on its severity. As organizations express concern about cyber-attacks and the hackers that perpetrate these attacks, there is increased interest in gaining insights into hacker’s activities against which organizations can protect, or for which capacity can be built. Researchers may also use the insights from this research to fine tune future information security research (Crossler et al. 2013). It is the hope that the implications of this research serves both research and practice.

ESSAY 2

JUST HOW RISKY IS IT ANYWAY?: THE ROLE OF RISK PERCEPTION AND TRUST ON CLICK-THROUGH INTENTION

2.1 Introduction

The Internet supports different services and functionalities, and has served as a mechanism for the delivery of services, communication and entertainment. Many individuals and organizations now depend on the Internet and applications (Keller et al. 2005; Knapp and Boulton 2006) such as search engines for business opportunities and information gathering. As a result, about 88 percent of adults in the US currently use the Internet, and spend more than 20 hours a week on the Internet (GO-Gulf 2015; Pew Research 2015). It is no wonder the Internet has become a popular attack vector for malware infections (Financial Services Rountable 2011). Attackers often use compromised or legitimately looking fake websites to distribute malware, making it difficult for users to detect (Abbasi et al. 2010). According to a recent vulnerability assessment by Symantec, malware was found on 1 in 566 websites (Symantec 2014). This supports the prevalence and elevated ranking of malware among the threats to cybersecurity: malware attacks rank highest (Computer Security Institute 2011). The financial impact of cybercrime is estimated at over $500 billion worldwide each year (Reuters 2014), and can cause business, personal and social damage (Dinev 2006). The impact of clicking through a link on the Internet that is malware infected can wreak havoc for the individual, including the stealing of private information (Dinev 2006) and storing surveillance software on the individuals computer in order to observe their behavior (Grazioli and Jarvenpaa 2000). Grazioli and Jarvenpaa (2003) argue that deceptions on the Internet threatens the sustainability of e-commerce. Attackers exploit search engine sites and e-commerce sites to distribute and spread malware. Given the consequences of clicking on a malware infected link, individuals may be discouraged from clicking on legitimate links and completing e-commerce transactions. Thus, endangering e-businesses that depend on click-through to complete online transactions (e.g. e-commerce, search engine results). Hence, in order to retain the Internet as a safe, efficient and effective platform for business transactions, it is important to understand how Internet users form their decisions to click-through URL links in a risky environment. Hence, this study addresses the research question: *"given a risky Internet environment what factors shape the individual's decision towards clicking through links on the Internet?"*

Our interest is in understanding why individuals click-through in the presence of the risks involved. We do so using the e-commerce transaction context, while specifically integrating malware risk perception, the risk propensity of using the Internet and computers, trust, familiarity and self-efficacy of information security as key determinants in online transactions. Using Sitkin and Pablo's (1992) theoretical framework in risky decision making, we show the factors affecting click-through intention. We find that the individual’s intention to click-through is significantly affected by their risk propensity, risk perception, trust of the site, familiarity and self-efficacy of information security.

The individual's interaction with Internet click-through and their perceptions around click-through is under-developed in IS research. Click-through is considered as both a reliable means for showing user preference (Joachims et al. 2005) and a behavioral response (Briggs and Hollis 1997). With respect to a person's decision process, clicks also depict a person's relative preference (Joachims et al. 2005). URL click-through has been used for customer referral, decision judgements, marketing and advertisements (Jansen et al. 2007). A click-through represents an implicit feedback and indicates relevance judgements, and has been used to measure advertising response and to indicate individuals’ immediate interest in a brand (Briggs and Hollis 1997). Thus, this study uses click-through intention to measure the individual's judgement towards a link. If URL links are perceived as unsafe, individuals may not click on them. This represents a huge loss for search engine companies (e.g. Google, Yahoo, and MSN) and e-commerce sites that depend on click-through for revenue (Jansen et al. 2007). Grier et al. (2010) found that 8% of 25 million URLs posted on Twitter point to malware sites, and suggests that about 0.13% of links on Twitter are clicked on; representing higher URL clicks than clicks from email spam.

Considering the prevalence of cybersecurity threats and the risks of malware on the Internet, studies investigating malware risks and Internet click-through are sparse. In addition, the coalescing of e-commerce and security research is an important aspect that requires further research. This study applies risky decision making theoretical framework to understand the individual's click-through intention. We also examine the effects of trust and familiarity on the individual’s intention, in the presence of these risks.

This study makes the following contributions to theory and practice. First, it proposes a research model and a set of theory-based hypotheses addressing why individuals click-through and what factors contribute to this behavior. Trust has been used extensively in e-commerce research to explain “how” and “why” individuals engage in e-commerce transactions, but has not been used in understanding risky decision making in the information security context. Second, our study answers the critical question of how trust affects secure behavioral intentions from a cybersecurity standpoint (Pfleeger and Caputo 2012). It does so by integrating trust in the risk framework and by applying the “where” aspects of theory building (Whetten 1989). The hope is that this research advances information security context-related research, and increases the importance and specificity of trust, risk and security research. In addition, this study provides insights for managerial practices that help enhance click-through of genuine and legitimate links on the Internet.

The rest of the essay is structured as follows. Section 2 reviews the conceptual and theoretical background of this research. Section 3 develops the research model and hypotheses. Section 4 describes the research method, measurement instruments, and data collection procedure. Section 5 presents the results. Section 6 then discusses the contributions, implications, limitations and finally the conclusion of this study.

2.2 Conceptual Background

Today, individuals' decision regarding clicking through URL links on the Internet for e-commerce transactions (Furnell 2004), information search, downloads and social media (Grier et al. 2010) is characterized as risky. Click-through is a behavioral response on the web that indicates immediate response (Briggs and Hollis 1997) or an action from a user (Richardson et al. 2007). In advertisement, click-through rate has been considered the best measure of advertising response on the Internet (Briggs and Hollis 1997). In terms of click-through in security, Akhawe and Felt (2013) found that users click-through Google chrome’s warnings about 70% of the time and that users who click-through also chose to remove a default setting on their computers. Thus, indicating the user’s cognitive choices. The study highlights the notion that click-through is an indication of individuals’ security behavior. When individuals click-through an insecure HTTP or link on a website, it can compromise the user’s session cookies, allowing an active attacker to hijack an individual’s session and steal confidential information or perpetrate other activities (Jackson & Barth, 2008). Most online social networks are targeted by malware where attackers have been known to experience higher click-through rates by luring individuals to click-through malware because of the individuals' perception of authenticity or shared content (Gao et al. 2011). In other words, the attacker takes advantage of the individuals' familiarity with the content. As search engine advertising becomes a significant part of internet browsing (Richardson et al. 2007), the importance and financial implications of click-through for online advertising giants such as Google and MSN cannot be underestimated. To the best of our knowledge, research that empirically evaluates the individual's click-through intention in an information security context is scarce. Hence, we believe that exploring the cognitive evaluations that individuals go through to click-through links on the Internet is an important and meaningful research from theoretical and practical viewpoints, especially as it concerns information security.

Given the rise of new technologies and mobile infrastructures, as well as the eager adoption and use of search tools, search volumes are expected to grow at an unprecedented scale (Im et al. 2016), and in turn increase click-through. Recent cybercrime activities have prompted individuals to consider security and privacy risks as they navigate the Internet and click-through several URLs. Criminals use links on e-commerce sites, even legitimate websites as attack vectors to attack individuals with malware, exposing individuals to credit card fraud, identity fraud, and unauthorized surveillance. Individuals not only evaluate the risks in e-commerce stemming from product defects, defecting retailers – which have been extensively researched in prior e-commerce studies (Featherman and Pavlou 2003; Kim et al. 2008; Pavlou 2003), but they also evaluate the risks that stem from Internet threats in e-commerce transactions, such as web-based malware, phishing, ransomware. In this study, risk in Internet click-through decision is defined as the extent to which there is uncertainty of potentially negative outcome from the decision to click-through a URL link in e-commerce and search engine platforms.

Sitkin and Pablo (1992) developed a risk decision model that has been used in many studies on decision making under risky situations (e.g., Chen et al. 2011; Cho and Lee 2006; Panzano and Billings 1997). The model posits that risk perception and risk propensity are strong determinants of risky behavioral intention. Risk propensity is defined as an individual's tendency to take or avoid risks (Sitkin and Pablo 1992). Individuals who have a high risk taking propensity are more likely to make risky decisions and take risky actions. According to Sitkin and Pablo (1992), risk propensity is a dynamic individual characteristic – a trait, which means that a person’s risk propensity may change over time. Risk perception is defined as an individual’s assessment of the risk inherent in a certain situation (Sitkin and Pablo 1992), in terms of the degree of uncertainty. The impact of risk perceptions on decision makers have been known to lead to uncertainty denial, overstatement or underestimation of risks, or even unjustified confidence in judgements. Sitkin and Pablo (1992) framework also posits that risk perception has a moderating effect on the relationship between risk propensity and risky behavior. The framework has been used in organizational and individual contexts and suggests that risk averse individuals will avoid risk as their perception of risk rises.

In order to explain the individual’s risky decision making in an e-commerce context, we extend risk framework to include trust as a determinant of click-through intention. Given that trust is a major determinant in an e-commerce environment and that this study intends to capture the individual’s behavioral intention in an e-commerce transaction context, we include trust in order to understand the role it plays in click-through behavior. There is established literature that supports and explains trust in online environments. The literature includes the dynamics of trust (Zahedi and Song 2008), trust and risk (Kim et al. 2008) , trust and product uncertainty (Gefen and Straub 2004), and trust and its various outcomes. By including trust, we examine the role that trust plays in inhibiting or encouraging risk based click-through decision. Gefen et al. (2008, p. 280) note that "…adding a trust perspective to other management information systems (MIS) theories could present intriguing and interesting insights…" Hence, we contribute to the trust literature by integrating trust in a cybersecurity risk environment.

2.3 Research Model and Hypotheses

Drawing upon the literature of risky decision making, we propose that risk propensity is a determinant of click-through intention. Adopting and extending Sitkin and Pablo (1992) risk framework to explore the impact of risk propensity on risk perception and behavioral intention, we propose that trust impacts risk perception and behavioral intention. Following past research, we also propose familiarity as impacting both trust and intention (Gefen 2000; Van Slyke et al. 2006). To clearly illustrate the proposed relationships, we formulate a nomological network to link malware risk severity as an antecedent of risk perception, and self-efficacy of information security as a determinant of intention (Rhee et al. 2009) . The constructs of interest are presented in Figure 2.1.

2.3.1 Computer Risk Propensity

Risk propensity has been defined as the individual's tendency to take or avoid risks (Sitkin and Pablo 1992). Specific to the use of computers and the Internet, and especially with the proliferation of Internet and computer based crimes, Chen et al. (2011) conceptualized risk taking propensity that focuses on risks inherent in using the Internet and computers. The use of computers and Internet indicate that individuals are vulnerable to threats related to computers and information systems. Hence, following Chen et al. (2011) we define computer risk propensity as an individual's tendency to take or avoid risks in the use of computers and the Internet. Malware infection have been known to compromise the security of information systems. Security of information systems consists of the protection of individuals' personal information with three goals; confidentiality, integrity and availability (Smith et al. 2011). Confidentiality requires that an individual's private information is restricted to only authorized users for authorized uses, integrity requires that such information remains unaltered, and availability requires that information is accessible to the user when it is needed and without delays.

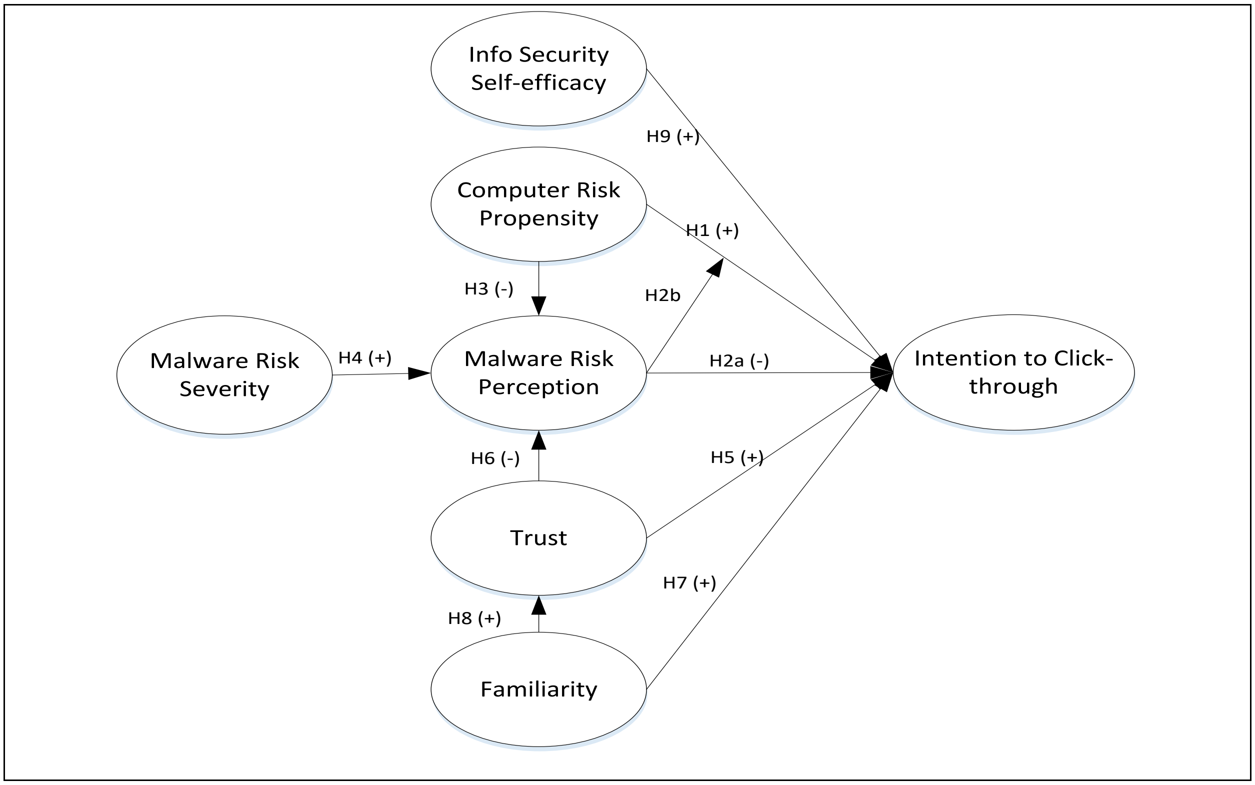

Figure 2.1: Conceptual Model (Essay 2)

Malware infection can lead to the loss of confidentiality, in which case an individual's private information such as credit card numbers, passwords, social security number, and medical information become available to unauthorized individuals. Integrity can also be compromised such that an individual's information is altered without their knowledge. Availability is affected when as a result of malware, the individual's computer becomes unusable and unavailable. However, given that individuals with high computer risk taking propensity are likely to engage in activities that are likely to encounter risks, these individuals are more likely to click-through potentially risky URL links when compared with individuals with low computer risk taking propensity. In this study, we argue that computer risk taking propensity is positively associated with an individual's tendency to click-through URL links on the Internet. Therefore, we hypothesize:

H1: Computer risk taking propensity positively influences click-through intention

2.3.2 Malware Risk Perception

Risk perception has been defined as a decision maker's assessment of the risk inherent in a situation (Sitkin and Pablo 1992), and involves the consideration of the context (Mayer et al. 1995). In this study, malware risk perception is defined as the individual's assessment of the risk of malware. Risk perception may lead individuals to deny the outcome, overestimate or underestimate the risks from malware. We posit that the outcome of the perception of risk is risk aversion (Sitkin and Weingart 1995). According to risk theory, the presence of risks will result in risk-averse tendencies in individuals (Sitkin and Pablo 1992). Malware risk involves the potential disruption of normal operations of computers or mobile devices. Malware is often used by criminals to monitor or control a user's online activities, steal personal information or access networks. Given that the human judgment is limited, resulting in the overestimating or underestimating of malware risks; a persons' subjective perception of the risk will influence their behavior. Risk perception has been studied in different situations with results consistently showing that risk perceptions influences attitudes and behavior (Dillard et al. 2012; Janz and Becker 1984; Keil et al. 2000). For example, an individual who thinks her computer system is vulnerable to or may be under some malware attack activity may exhibit negative attitude towards malware, and an aversion towards a risky behavior. Malware risk perception is expected to have a negative influence on behavioral intention. Risk framework posits that risk perception negatively influences willingness to carry out risky behavior (Sitkin and Pablo 1992), and other studies provide support for the relationship between risk perception and behavioral intention (Chen et al. 2011). Hence, given that clicking through links is considered risky, malware risk perception is likely to negatively affect an individual's intention to click-through. Therefore, we hypothesize:

H2a: The higher the malware risk perception, the lower the click-through intention

We expect that the relationship between computer risk taking propensity and click-through intention will be moderated by malware risk perception, making it weaker. Only when risk is present does risk propensity influence decision making. Therefore, when an individual does not perceive malware risk, the influence of risk propensity on click-through intention may be non-existent. However, when an individual has a high perception of malware risks, then their computer risk propensity may influence click-through intention, making it weaker. Therefore, we hypothesize:

H2b: The positive relationship between computer risk taking propensity and click-through intention will be weaker with malware risk perception

Furthermore, we argue that computer risk taking propensity impacts malware risk perception. An individual's risk taking propensity may lead them to limit the links that an individual is willing to click-through. Additionally, their risk propensity may alert them to the risks inherent on the Internet or on clicking through links that may lead to undesired results. Sitkin and Weingart (1995) support this notion when they suggest that risk propensity can influence the relative salience of situational threats (e.g. cybercrime, malware infection) and that this leads to a biased perception of risk. For example, an individual with low computer risk taking propensity (i.e., risk–averse, risk avoiding), "...is more likely to attend to and weigh negative outcomes, thus overestimating the probability of loss relative to the probability of gain. As a consequence, a risk-averse decision maker tends to overestimate the level of risk inherent in a decision situation'' (Sitkin and Pablo 1992, p. 19) . Conversely, individuals with high computer risk taking propensity (i.e., risk seeking) are more likely to give more weight to positive outcomes, and therefore overestimate the possibility of gains than losses (i.e., underestimate the risks of malware). Cho and Lee (2006) found that individuals with higher risk-taking propensity concerning investment decisions tend to have a lower risk perception towards stock market investments. As did Keil et al. (2000), in their study of software project where they found that risk-taking managers tend to perceive lower levels of risk than managers who are risk averse. Therefore, we hypothesize:

> H3: The higher the individual's computer risk taking propensity, the lower the level of malware risk perception

2.3.3 Malware Risk Severity

We posit that an individual's perceived severity of malware risk determines their assessment of the risk. Existing evidence (e.g., Herath and Rao 2009b; Liang and Xue 2010) concerning the effect of severity of Internet and computer based threats (e.g. security breaches, malware, spyware) suggests that as the severity of risk increases, the likelihood that decision makers will have higher perception of risk increases correspondingly. Risk based decision literature also suggests that risk severity affects an individual's assessment of risks (Fischhoff et al. 1978; Mitchell 1999). Prior studies in information security protective behaviors have defined perceived severity as the degree of harm associated with a threat (Herath and Rao 2009b), and the extent to which an individual perceives that negative consequences caused by a malicious technology will be severe (Liang and Xue 2009). In relation to sanctions, severity has been defined as the degree to which the sanction is perceived as harsh or problematic (Johnston et al. 2015).

Following prior studies, we therefore define malware risk severity as the degree of harm associated with malware risks (Herath and Rao 2009b). When an individual believes that the harm associated with malware is insignificant, it is more likely that their perception of risk will be reduced. Conversely, when an individual believes the harm associated with malware is significant, their perception of risk increases. Workman (2007) notes that one's assessment of risk is based on the severity and cost of the damage associated with a threat. Thus, individuals who have a high perception of the severity of malware (e.g. loss of private information due to malware infection), will more likely have a high level of malware perception. In other words, the individual sees the potential harm from malware risk as significant. Therefore, we hypothesize:

> H4: The higher the individual's malware risk severity, the higher the level of malware risk perception

2.3.4 Trust

Over a decade of e-commerce research in information systems (Mayer et al. 1995; Pavlou and Gefen 2004; Zhou et al. 2009) identifies trust as a major determining factor in behavioral intentions. Trust is unquestionably an integral part of social interaction, allowing individuals to act under the risk of negative consequences (Artz and Gil 2007). However, with recent growth in cybercrimes, a question that must now be asked is this: how does trust affect secure behavioral intentions (Pfleeger and Caputo 2012)? Thus, leveraging what we know about trust and purchase behavior in the e-commerce environment, we explore the effect of trust in terms of secure behaviors.

Trust has been defined in many ways, including the expectation that the trustee will behave ethically (Hosmer 1995), behave in a dependable manner, and also as a factor in the presence of uncertainty (Gefen 2000; Mayer et al. 1995). Trust refers to the belief or willingness to believe that one can rely on the fairness, goodness, strength, and ability of another (Fukuyama 1995). Trust has also been described as both a complex and multi-dimensional construct with many inter-related aspects that include its trusting beliefs – competence, benevolence, and integrity, as well as its trusting intentions – the willingness to depend (Gefen 2000; McKnight et al. 2002). McKnight et al. (1998) define trust as an individual's beliefs about the extent to which a target is likely to behave in a way that is benevolent, competent, honest, or predictable in a situation. Building on a combination of earlier trust definitions and using the context of this study, we define trust in a website as an individual's subjective belief about the extent to which the website is likely to behave in a way that is benevolent, competent, reliable or predictable in a situation.

The willingness to depend refers to an individual's volition to be vulnerable to another (McKnight et al. 2002). That is, the individual's conscious choice to cast aside doubts and proceed with a relationship with another (Holmes 1991). In the context of click-through, when an individual is willing to depend on a website, then the individual "… is more likely to accept the specific vulnerabilities associated with using the site" (McKnight et al. 2002, p. 303). Hence, individuals assured of a website's dependable manner will develop a reduced notion of uncertainty and click on links displayed on the website. An individual who has developed a higher level of trust in a website (e.g. Amazon.com, search engines like Google, Bing, Yahoo!), is more likely to click on links on the website in order to go about their business. Based on these arguments and previously tested relationship between trust and intention (Kim et al. 2009; Pavlou 2003; Pavlou and Gefen 2004), we expect that trust in a website will influence the individuals' intention to click-through links on such website. Therefore, we hypothesize:

H5: Trust positively influences intention to click-through

The relationship between trust and risk perceptions has been given much attention in e-commerce and trust literature (e.g., Gefen et al. 2003; Kim et al. 2008; Pavlou 2003). The view from the literature suggests that decision makers in a risky situation will hedge against uncertainty by engaging trust. The notion is that risk perception is a situational factor that necessitates trust. That is, trust only arises in risky situations (Mayer et al. 1995). Thus, an outcome of trust is the reduction in risk perception. When an individual trusts an online vendor or a website in which he or she is transacting, it is likely that the individual's perception of malware risk is reduced. It is expected that individuals would rarely transact with websites/online vendors known to have malware infection. Hence, the trust the individual has of the website should reduce the perception of malware risk. Therefore, we hypothesize:

H6: Trust negatively influences malware risk perception

2.3.5 Familiarity

Familiarity has been defined as an individual's understanding of another's behavior based on prior experiences (Bhattacherjee 2002). Following this definition, we refer to familiarity as the individual's understanding of the website based on the individual's prior experience of the website. For example individuals who have developed a favorable understanding of an e-commerce site and as a result estimated their likelihood of a desired future favorable behavior (Bhattacherjee 2002; Gefen 2000) will form a relationship with the site. This relationship tends to reduce the uncertainties the individual may have, and influence the individuals' trust in the website. Hence, familiarity is an antecedent of trust (Gefen 2000). We expect that the effects of familiarity in e-commerce context extend to information security contexts. A common notion in the proliferation of fake websites and phishing attempts that seek to entice individuals to divulge their private information, is that these fake website are created to look very similar to the ones the individual is familiar (Abbasi et al. 2010; Sasse and Kirlappos 2011). When an individual is at a fake website that looks very similar to the one s/he had previously transacted, the individual's familiarity may lead them to trust this site (even though may be fake).

We also expect that familiarity will influence intention to click-through (Van Slyke et al. 2006). Similar to the e-commerce context, an individual who is familiar through previous interactions with a website will tend to trust the site, and click through links on the website. In the same vein, attackers may exploit the individual's familiarity with websites to entice click-through, distribute malware, and extract individuals' private information (Sasse and Kirlappos 2011). Consistent with previous studies that have tested the relationship between familiarity, trust and intention (Bhattacherjee 2002; Gefen 2000; Van Slyke et al. 2006) we hypothesize:

H7: Familiarity positively influences intention to click-through

H8: Familiarity positively influences trust

2.3.6 Self-Efficacy of Information Security

Self-efficacy is a determinant of individual behavior (Bandura 1998). When an individual has a high level of self-efficacy, they tend to have a strong sense of their ability to perform a task. Derived from the general concept of self-efficacy, computer self-efficacy (CSE) refers to one's efficacy beliefs involving diverse computer applications and domains. CSE is defined as an individual's judgment of their capability to use a computer (Compeau and Higgins 1995). Previous studies have validated its effect on many computers related behaviors (Chang et al. 2015; Hong et al. 2013; Venkatesh et al. 2003). Agarwal et al. (2000) and Compeau and Higgins (1995) have since argued for the importance of exploring specific concepts of CSE. They also argued for the necessity to be more precise in the definition of the study domain. Hence, Rhee et al. (2009) proposed and validated the specific concepts of CSE in the domain of information security, named self-efficacy of information security. Self-efficacy of information security (SEIS) is defined as the individual's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction (Rhee et al. 2009). This form of self-efficacy is manifested when individuals believe that they can accurately assess information security risks related to malware. When individuals believe in their capabilities to identify websites with malware, or their ability to handle issues that arise as a result of malware, it is plausible that this belief can influence their decision to click-through links on the website. Rhee et al. (2009) found that SEIS is positively related to behavioral intention. On the basis of this previously tested relationship, as well as other specific concepts of CSE on intention (Chang et al. 2015), we expect that SEIS will influence the individuals' intention to click-through. Therefore, we hypothesize:

H9: Self-efficacy of information security positively influences intention to click-through

2.4 Research Methodology

This study employed a scenario-based survey to test our model. We developed hypothetical scenarios (Weber 1992) describing shopping situations and a questionnaire based on the situations. See Appendix B2. Scenario-based techniques, also known as vignettes "... present subjects with written descriptions of realistic situations and then request responses on a number of rating scales that measure the dependent variables of interest" (Trevino 1992, pp. 127–128). Other studies have used similar techniques to empirically test their models (Malhotra et al. 2004; Webster and Trevino 1995), and most especially for testing behavioral intentions in situations involving ethics and computer abuse (D'Arcy et al. 2009; Siponen and Vance 2010), software piracy issue

(Moores and Chang 2006), privacy concern (Malhotra et al. 2004). For example, in their study, Siponen and Vance (2010) used a hypothetical scenario-based survey method to ascertain the employee's violation of security policy. The scenario method affords many advantages for research, especially research on behaviors that may be deemed undesirable. First, scenarios integrate specific situational facts that are important in decision making geared towards deviant behaviors in a manner that survey questions that do not reference situations are unable (Siponen and Vance 2010). Second, scenarios provide an indirect way to measure intention to perform behaviors that that may be unexpected or unethical, which are difficult to directly measure because respondents may want to respond in a socially desirable manner (Trevino 1992).

2.4.1 Scenario Design

In order to generalize our findings to many Internet environments, we developed two hypothetical scenarios describing different situations. Each survey includes a scenario and subsequent questions. In each survey, respondents are instructed to read the scenario and complete the questionnaire. The first scenario-based survey (A) considers Amazon.com as the source site, while the second scenario-based survey (B) considers a generic search engine site as a source site, where respondents were asked to select a search engine site of their choice. Studies have shown that search engines are effective at returning relevant listings for e-commerce search (Jansen et al. 2007). In addition, previous studies have utilized similar scenario approaches. For example, Pavlou (2003) designed multiple surveys with scenarios to test e-commerce adoption, where respondents in one group complete a survey based on Amazon.com, and another group was based on a selected web retailer of their choice. The rationale behind the use of different scenarios with predetermined and self-selected sites is to test several contextual bases in order to assess its robustness and generalizability across targets (Pavlou 2003). Given that Amazon has been heavily used in several e-commerce studies (e.g., Gefen 2000; Pavlou 2003), we designed these two scenarios to access whether click-through intention differs on the basis of trust of the source sites and malware risk perception. In administrating the scenario-based survey, a survey link was made accessible to respondents, so that when clicked, one of the scenario-based surveys is presented to the respondents. The determination of which of the scenario-based surveys (A) or (B) is presented to the respondent was based on time of day. For example, if respondents click on the survey link in the morning, scenario-based survey A is presented, and if in the evening, then B is presented.

2.4.2 Measurement

All the measurement scales have been used and validated in previous research, and all constructs used a minimum of three measurement items. In addition, all constructs were measured on a 7-point Likert scale. All measurement items are included in Appendix B1. The dependent variable, click-through intention (INT) was measured using five items adapted from Davis (1989) and Ajzen (1991). The items assessed whether respondents intend to click-through URL links to websites suggested to them by the source site, and whether they would purchase from the target site that was suggested by the source site. The notion is that the respondent's intention to purchase the item also means that the respondent will click-through in order to do so. Other items accessed the individual's risk propensity (PRO), their risk perception (PER), trust (TRU) of the source site, perception of risk severity (SEV), familiarity (FAM), and self-efficacy of information security (SEIS). In addition to the items measuring the latent constructs, we captured appropriate demographic variables including age, gender an education level.

Prior studies have shown that age (Gardner and Steinberg 2005) and gender (Jianakoplos and Bernasek 1998; Sunden and Surette 1998) may influence risky decision making. Therefore, in order to exclude the variance explained by age and gender, we control for their influence on click-through intention. In addition, since data was collected from two different scenarios, we control for the influence of type of scenario. This was done following previous information security studies that employed scenarios (e.g., Vance et al. 2012b). The instrument was pretested with graduate business students, where students were asked to review the instrument and make comments about any items that seemed ambiguous or incomplete. The test revealed that questions related to trust of website and intention needed changes to improve clarity.

2.4.3 Data Collection

Primary data for this study was collected from students from a large university in southwest of the United States, through an online survey engine. Students voluntarily participated in this study in exchange for course credit. Since students represent a large population of the Internet users, who are as susceptible to potentially malicious links as any other individual using the Internet for searches and purchases. Their perceptions and behavioral intentions provide valuable insight into the research questions of this study. Data collection was done over a two-week time period.

The questionnaires received 401 responses: 205 and 196 for scenarios A and B respectively. Fifty responses were deleted for reasons including incomplete responses and same answer to all questions (e.g. all 7's). The final sample consisted of a valid 347 responses. The samples' demographic distribution is presented in Table 2.1. The sample depicts that a majority, 69% of the student sample also work full time or part time while attending school.

Table 2.1: Demographic Distribution of the Sample (Essay 2)

Variables	Options	Percentage
Gender	Male	55.3
	Female	44.7
Age	Less than 21	28.2
	21- 25	53.6
	26 - 30	9.5
	31- 35	4.6
	36 and above	4
Highest education completed	High school	73.2
	Bachelors	26.8
Work Status	Full time	21
	Part time	49
	Do not work	30

2.5 Data Analysis and Result

2.5.1 Measurement Model Analysis

Using Wilks's lambda, the results of the two groups were similar and statistically inseparable. (T-tests reveals that there were no significant differences between the groups on any constructs in the model. Therefore, the data was combined for an inclusive statistical analysis. Partial least square (PLS), specifically SmartPLS Version 2.0 was used in this study. To investigate the adequacy of the measures, reliability, convergent validity, and discriminant validity of the instruments were examined. Table 2.2 shows the descriptive statistics, while Table 2.3 shows the result of an exploratory factor analysis, where all loadings are larger than the suggested threshold of 0.70 (Chin 1998). Table 2.4 shows that all the composite reliabilities are larger than the suggested value of 0.70 and all AVE values are greater than the suggested 0.50, indicating a good convergent validity and measurement model.

Table 2.2: Descriptive Statistics (Essay 2)

	Mean	S.D.
Intention to click-through (INT)	3.830	1.425
Malware risk perception (PER)	4.471	1.373
Computer risk propensity (PRO)	3.441	1.754
Malware risk severity (SEV)	4.626	1.332
Trust (TRU)	4.737	1.318
Familiarity (FAM)	5.368	1.296
Self-efficacy (SEIS)	4.152	1.432

Note: constructs are seven-point scales

Discriminant validity is reached if AVE for each construct is greater than the variance shared between the construct and other constructs in the model (Chin 1998), and if the items load more strongly on their constructs. The values in Table 2.3 indicate that discriminant validity was attained. To assess the multicollinearity of the constructs, variance inflation factor (VIF) statistics was examined to ensure they are lower than the suggested 3.3 (Diamantopoulos 2006). The VIF values for four indicators of INT, which are PER, PRO, TRU, FAM, and SEIS are 1.14, 1.07, 1.3, 1.26, and 1.12 respectively. Hence, desired low multicollinearity was observed.

To access the common method bias, we performed Harman's single factor test (Podsakoff et al. 2003). All the variables were loaded into exploratory factor analysis (EFA) without rotation. Evidence for common method bias exists if one factor accounts for most of the covariance in all factors. Since no single factor accounted for the majority of the covariance, this suggests that common method bias is not an issue.

Table 2.3: Exploratory Factor Analysis (Essay 2)

Construct	PRO	INT	FAM	TRU	SEIS	SEV	PER
PRO1	.816	.103	-.050	.018	.067	.073	.052
PRO2	.927	.016	-.029	-.017	.052	.093	.051
PRO3	.931	.036	.004	-.037	.058	.100	.075
PRO4	.933	.063	.010	-.039	.090	.083	.085
PRO5	.936	.062	.028	-.019	.098	.108	.081
PER1	.105	-.141	.040	-.113	.092	.139	.848
PER2	.140	-.088	.078	-.098	.096	.197	.879
PER3	.070	-.092	.061	-.023	.064	.237	.836
SEV1	.090	-.042	.066	.015	-.010	.853	.141
SEV2	.068	-.092	.123	.053	.029	.889	.108
SEV3	.101	.036	.038	-.063	-.027	.888	.112
FAM1	-.055	.044	.874	.171	.108	.093	.037
FAM2	-.004	.135	.887	.106	.078	.076	.003
FAM3	-.019	.018	.868	.238	.052	.111	.045
FAM4	-.022	.057	.869	.241	.084	.068	.067
FAM5	.066	.370	.704	.059	.063	-.064	.065
TRU1	-.009	.254	.171	.778	.041	.020	-.083
TRU2	-.035	.168	.199	.904	.080	-.028	-.058
TRU3	-.018	.156	.202	.904	.118	-.043	-.058
TRU4	-.033	.118	.218	.902	.120	-.021	-.065
INT1	.026	.853	.171	.168	.006	.033	-.048
INT2	.019	.870	.169	.173	.014	.041	-.068
INT3	.067	.888	.105	.132	.071	.069	-.051
INT4	.083	.831	.020	.102	.149	-.044	-.106
INT5	.093	.847	.037	.109	.143	-.078	-.073
SEIS1	.096	.134	.038	.093	.834	-.035	.004
SEIS2	.079	.118	.037	.099	.878	-.036	.011
SEIS3	.091	.087	.139	.058	.824	-.041	.073
SEIS4	.059	.002	.111	.061	.811	.020	.147

Table 2.4: Reliability, Correlation, and Discriminant Validity of Constructs (Essay 2)

	CR	Alpha	AVE	FAM	INT	PER	PRO	SEV	SEIS	TRU
FAM	0.953	0.935	0.835	0.913						
INT	0.947	0.930	0.783	0.225	0.885					
PER	0.927	0.882	0.810	0.103	-0.175	0.900				
PRO	0.965	0.955	0.850	-0.009	0.122	0.211	0.922			
SEV	0.898	0.829	0.745	0.151	0.026	0.388	0.249	0.864		
SEIS	0.903	0.865	0.700	0.192	0.198	0.150	0.186	-0.03	0.836	
TRU	0.956	0.938	0.845	0.409	0.367	-0.159	-0.035	-0.05	0.204	0.919

Note: CR: Composite Reliability, AVE: Average Variance Extracted, Diagonal Elements (in bold font) are Square Root of AVE

2.5.2 Structural Model Analysis

The results of the structural model and hypotheses testing are presented in Figure 2.2 and Table 2.5, respectively. The hypotheses in the model are evaluated and interpreted using results from path coefficients, and t-values. The model explains 24 percent of the variance in click-through intention. The model also explains 18 and 17 percent of the variances in malware risk perception and trust respectively. Computer risk propensity has a significant effect on click-through intention ($\beta = .14$, $p<0.01$), thus rendering support for hypothesis 1. Malware risk perception has a negative and significant effect on click-through intention ($\beta = -.23$, $p<0.001$), therefore hypotheses 2a is supported. We also found that the moderating effect of malware risk perception ($\beta = .02$) between computer risk propensity and click-through intention was not significant. Hence, hypothesis 2b is unsupported. The relationship between computer risk propensity and malware risk perception is significant ($\beta =.12$, $p<0.05$), but surprisingly had an opposite effect; we found that the effect is positive rather than the hypothesized negative effect. Therefore, hypothesis 3 is unsupported.

Malware risk severity has a significant positive effect on malware risk perception (β =.35, p<0.001), hence hypotheses 4 is supported. Trust also has a significant effect on click-through intention (β = .27, p<0.001). Hence, hypotheses 5 is supported. Trust has a negative and significant effect on malware risk perception (β = -.14, p<0.05), therefore, hypotheses 6 is supported. The relationships between familiarity (β =.19, p<0.01) and click-through intention, as well as familiarity (β =.42, p<0.001) and trust are positive and significant. Therefore, hypothesis 7 and 8 are supported. We also found that self-efficacy of information security (β =.11, p<0.05) has a positive and significant effect on click-through intention. Hence, hypothesis 9 is supported.

In the case of the control variables, gender (β = -.03) and age (β = .07) do not have significant effects on click-through intention. However, scenario type (β =-.13, p<0.01) was found to have a significant effect on click-through intention.

Table 2.5: Results of Hypothesis Tests (Essay 2)

Hypotheses	Result
HI: Computer risk propensity → click-through intention (+)	Supported
H2a: Malware risk perception → click-through intention (-)	Supported
H2b: Malware risk perception moderates the relationship between risk propensity and click-through intention	Not Supported
H3: Computer risk propensity → Malware risk perception (-)	Not Supported (Contradicted)
H4: Malware risk severity → Malware risk perception (+)	Supported
H5a: Trust → intention to click-through (+)	Supported
H6: Trust → Malware risk perception (-)	Supported
H7: Familiarity → click-through intention (+)	Supported
H8: Familiarity → Trust (+)	Supported
H9: Self-efficacy of information security → click-through intention (+)	Supported

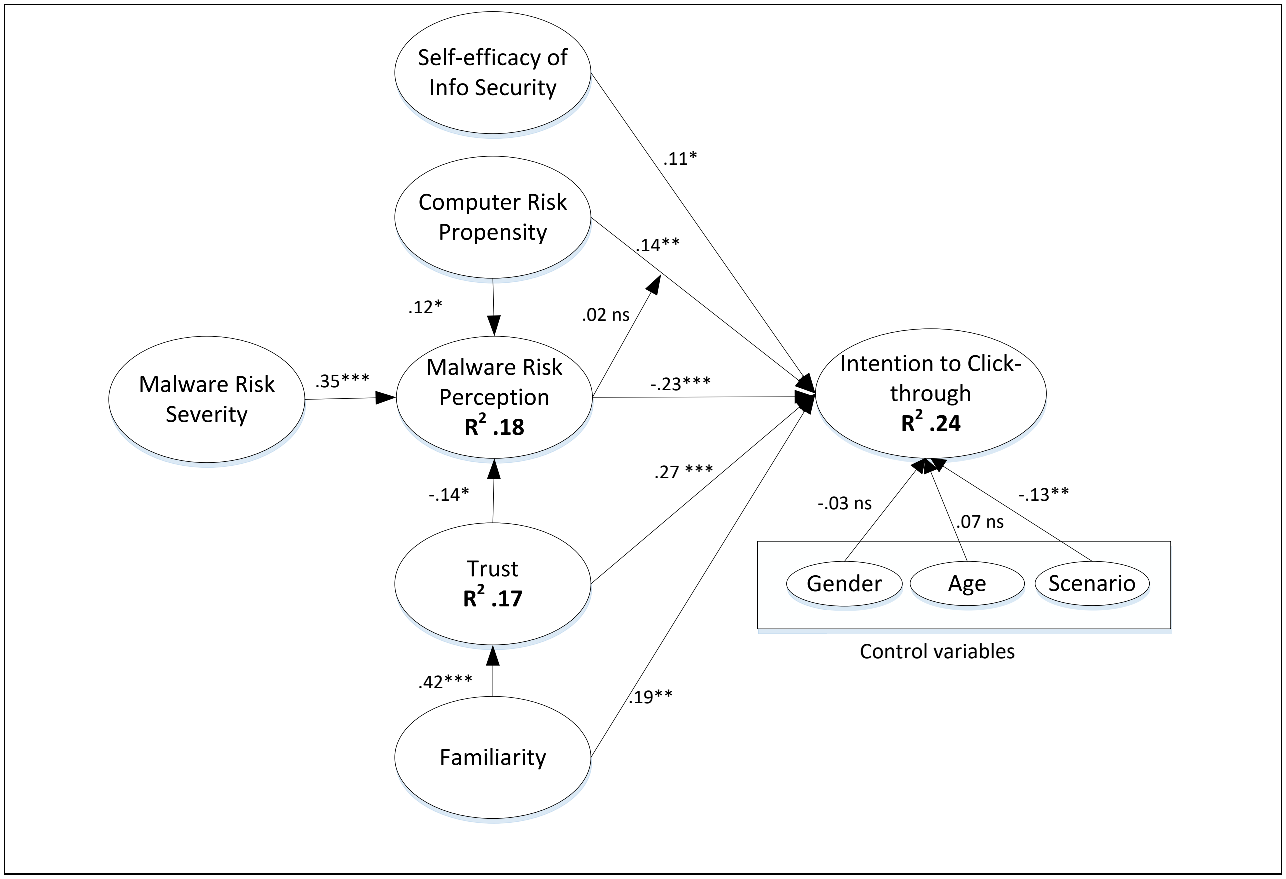

Figure 2.2: Structural Model (Essay 2)

Note: Model 1(combined model); * Significant at the 0.05, ** significant at the 0.01 level, *** significant at the 0.001 level, ns not significant

2.5.3 Multi-Group Analysis

To test the generalizability of the model, we performed a multi-group analysis. To perform a multi-group analysis of the model we separated the groups based on the scenarios (Model 2: Amazon.com scenario and Model 3: the self-selected search engine site scenario). Since each group is analyzed separately from the other in the multi-group analysis, we did not control for scenario type. Table 2.6 displays the results between models 1, 2, 3, and the effect of the constructs on malware risk perception, trust, and click-through intention as the dependent variables in this study. Model 1 is the combined sample which holds both the Amazon.com and the search engine groups (n = 347). Model 2 is the Amazon scenario group only (n= 188), while model 3 is the search engine scenario group (n= 159). To compare Model 2 with Model 3, the results of the structural model testing are depicted in Figures 2.3 and 2.4, respectively. The results show that the model constructs explained a slightly larger amount of variance of click-through intention for group 2 (25%) than for group 3 (23%). In addition, there are interesting differences between the groups with respect to the strengths of the relationships between malware risk perception, computer risk propensity, and intention. For example, the strength of relationship between malware risk perception and intention is stronger in Model 3 than in Model 2. This means that in the search engine scenario, individuals expressed more perception of malware risk. Also, the strength of relationship between computer risk propensity and intention is stronger in Model 2 than in Model 3. This suggests that in Model 3, the propensity for risk was not strongly considered in the individual's decision to click-through.

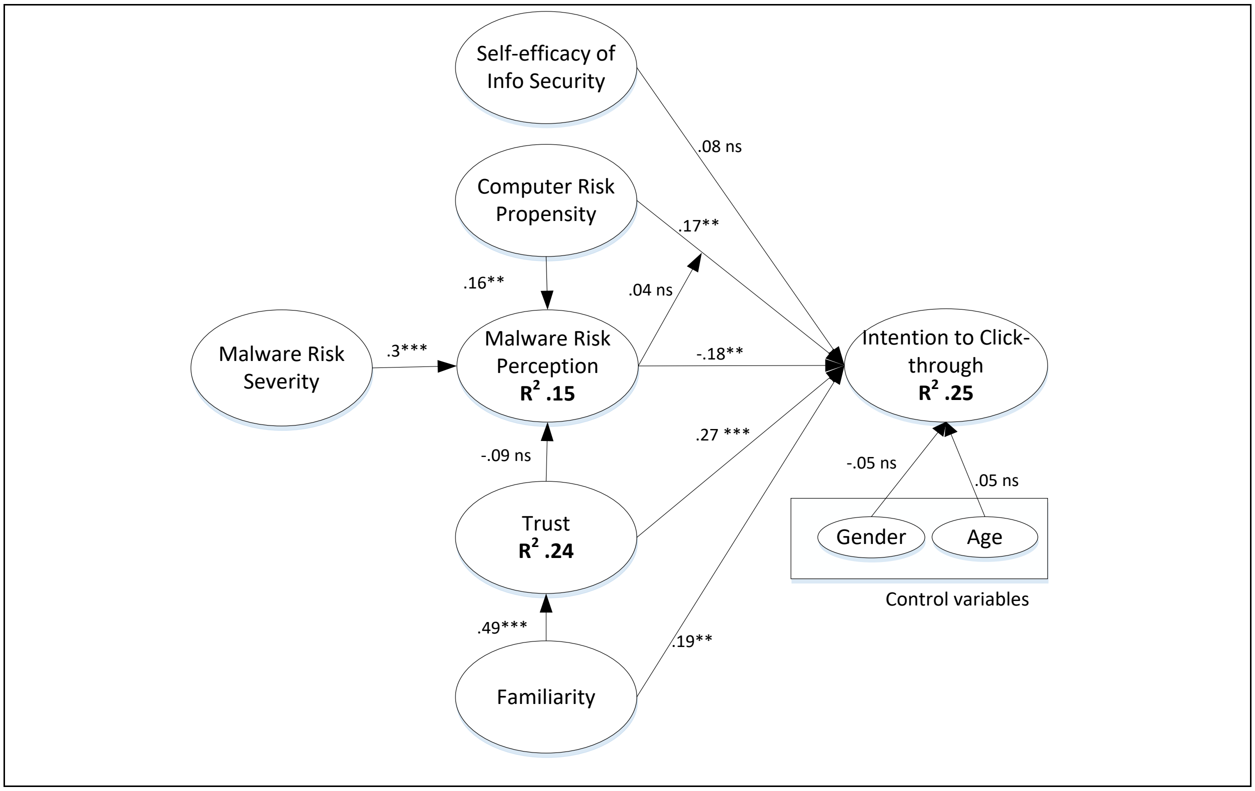

Figure 2.3: Amazon Scenario (Essay 2)
Note: ***p < 0.01 (|t| > 2.58), **p < 0.05 (|t| > 1.96), *p < 0.10 (|t| > 1.65)

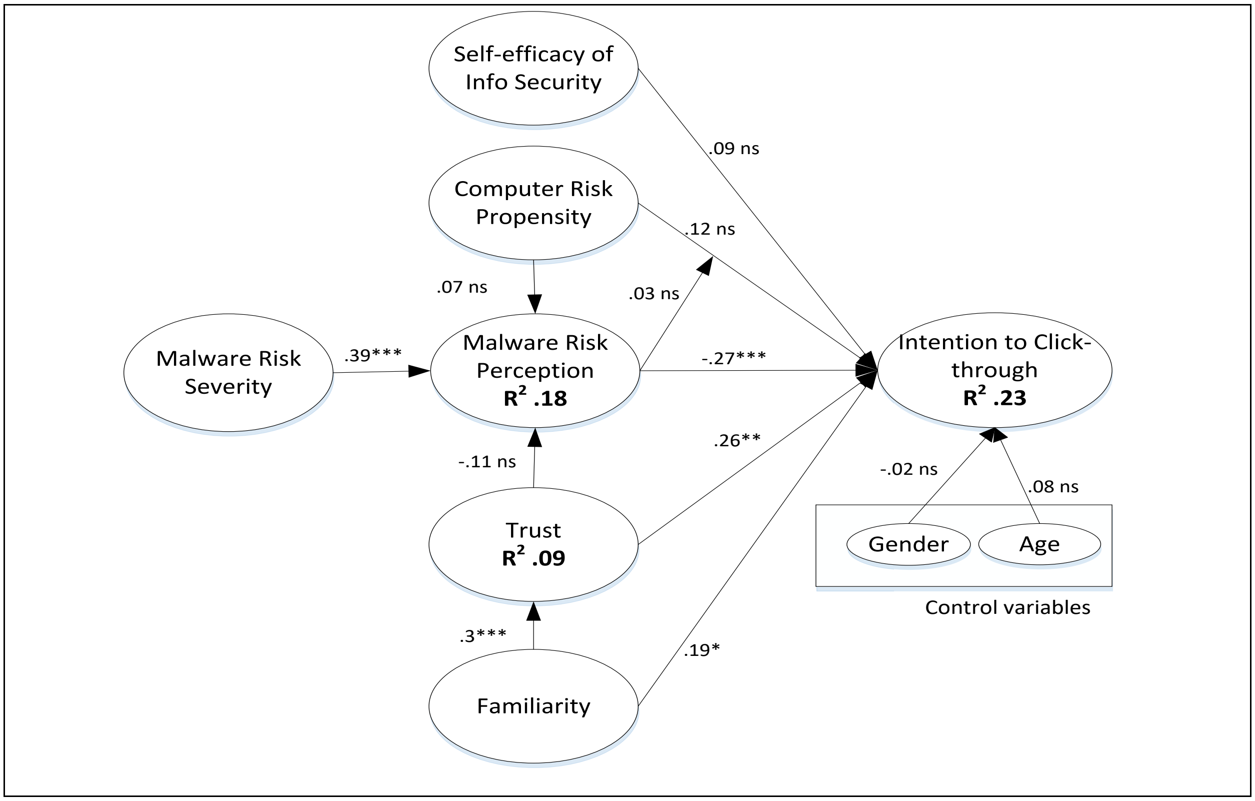

Figure 2.4: Search Engine Scenario (Essay

Note: ***p < 0.01 (|t| > 2.58), **p < 0.05 (|t| > 1.96), *p < 0.10 (|t| > 1.65)

Table 2.6: Summary of Data Analysis Results (Essay 2)

	Trust			Malware Risk Perception			Click through-Intention		
Independent Variables	Model 1	Model 2	Model 3	Model 1	Model 2	Model 3	Model 1	Model 2	Model 3
Gender							-0.03	-0.05	-0.02
							(0.52)	(0.69)	(0.30)
Age							0.07	0.05	0.08
							(1.51)	(0.96)	(1.15)
Scenario							-0.13***		
							2.59		
PRO				0.12**^	0.16**^	0.07^	0.14	0.18**	0.12
				(2.14)	(2.14)	(0.84)	(2.69)	(2.31)	(1.60)
PER							-0.23***	-0.18**	-0.27***
							(3.97)	(2.26)	(3.59)
SEV				0.35***	0.30***	0.38***			
				(5.67)	(3.71)	(4.03)			
TRU				-0.14**	-0.09	-0.11	0.27***	0.27**	0.26**
				(2.41)	(1.09)	(1.48)	(3.74)	(2.59)	(2.56)
FAM	0.42***	0.49***	0.30***				0.18***	0.19**	0.19*
	(8.02)	(6.73)	(3.64)				(3.16)	(2.33)	(1.96)
SEIS							0.11*	0.08	0.09
							(2.01)	(1.01)	(1.03)
PRO * PER							0.01	0.03	0.04
							(0.80)	(0.32)	(0.44)

Note: Each cell contains beta, and t-statistic in parentheses. ^ Opposite behavior. ***p < 0.01 (|t| > 2.58), **p < 0.05 (|t| > 1.96), *p < 0.10 (|t| > 1.65)

2.6 Discussion

The Internet and its functionalities such as e-commerce and search engine represent major access points endangered by cybersecurity threats such as malware distribution through URL links. Based on the results of this study, we argue that users form beliefs about websites with which they transact based on their individual characteristics, the social contexts and trust. Drawing from the literature in both risk based decision making and trust in online transactions, we argue that computer risk propensity, malware risk perception, trust, and familiarity are likely to create a significant influence. These factors are posited to not only have direct impacts but they are also related with each other in developing click-through intention. In addition, we argue that an individual's belief in their self-efficacy of information security directly affects their intention to click-through in the face of risks. Further, malware risk severity and familiarity are important antecedents to malware risk perception and trust, respectively.

2.6.1 Findings of the Study

Through empirical evaluation, we find support for most of the relationships on our proposed model. The results show that computer risk propensity is positively associated with click-through intention, while malware risk perception reduces intention to click-through. Our study finds that the individual' risk propensity influences how they make decisions regardless of how they perceive inherent malware risks. In other words, the direct link between risk propensity and click-through intention suggests that although individuals are aware of potential risks in clicking through links on the Internet, they still choose to accept the risk in clicking through URL links.

Surprising, we find a contradictory relationship between malware risk propensity and malware risk perception. We hypothesized that risk propensity reduces risk perception. However, we find the opposite relationship, where risk propensity seems to be significant in increasing risk perception. Keil et al. (2000) note that in conditions where individuals may have developed conservative and lower limits for risk perception, the result is that both individuals with high risk propensity and those with low risk propensity exhibit high risk perception. Another explanation for the contradictory result is the possibility that a high risk taking propensity may actually increase one's perception of that risk. For example, an individual that exhibits high risk taking propensity and who performs high risk sports (e.g. bungee jumping), may have a higher perception of the risks involved in the sport (e.g. death, rope breakage, injury etc.); more so than an individual who is averse to the sport.

We find evidence that malware risk severity significantly increases malware risk perception. We also find that the trust individuals have of the websites (Amazon.com and search engine) influences click-through intention. In addition, we find that trust also reduces the perception of malware risk that an individual has. This result supports previous studies in trust, risk and transaction intention (McKnight and Chervany 2001; Van Slyke et al. 2006). Familiarity was found to have a significant effect on click-through intention. Such that individuals who are familiar with certain websites are more likely to click-through links on the sites. This result supports Gefen (2000) and Bhattacherjee (2002) who argue that familiarity with the website is a key factor in not only trust but behavioral intention. In addition, we find evidence that self-efficacy of information security increases click-through intention.

Our results show that malware risk perception does not mediate the relationship between computer risk taking propensity and click-through intention. Thus, the effect of risk propensity on click-through intention is direct and not mediated by malware risk perception. This lack of mediation effect suggests that individuals' risk propensity is not taken into consideration as individuals contemplate click-through. An explanation for this result may be that click-through behavior is driven by the need or intensity with which the individual enters the e-commerce or information search environment (i.e., goal directed) (Venkatesh and Agarwal 2006) prompting individuals to take the risk. Wolfinbarger and Gilly (2001) note that when there is a goal-oriented need, individuals tend not to linger. Rather, they execute their online transactions (e.g. purchase) quickly. Although the individuals in this study were given a scenario, the scenario did include a task. Hence, we suspect their goal-orientation may have prompted the (effect observed) lack of consideration for risk propensity. In terms of the non-significant moderating effect of malware risk perception between computer risk propensity and click-through intention, a possible explanation may be that risk propensity does not depend on one's perception of risk. Such that individuals tend to accept risks irrespective of their perception of risks.

Considering the control variables, gender and age have little influence on click-through intention. A possible explanation is that the judgement of click-through intention in an information security domain is done irrespective of gender and age differences. Thus, consistent with prior findings suggesting that demographics variables explain a small amount of choice behavior (Gupta et al. 2004; Quelch and Klein 1996). However, scenario type was found to have a significant and negative effect on click-through intention.

In terms of the multi-group analysis, we find key differences in the influences exerted by trust, malware risk perception, and computer risk propensity on click-through intention. In model 2 (i.e., Amazon.com), trust is not significant in its relationship to malware risk perception. One explanation for this effect may be that individuals in the Amazon.com scenario have more trust for Amazon such that they do not care so much about the risk of malware while shopping at the online retailer. This result is consistent with suggestions that trust is only effective when there is high concern over risks (Gefen et al. 2003; Mayer et al. 1995). In addition, Zahedi and Song (2008) note that although trust is crucial in online transactions, its importance diminishes over time as people learn about those with whom they interact. Hence, the importance of trust as a key consideration decreases with experience, and changes over time.

In model 3 (i.e., the self-selected search engine), the results show that trust is also not significant in its effect on malware risk perception. Given that individuals may have selected a search engine with which they have developed some level of trust, the relative concern for risk is diminished. However, it is worth noting that the strength of the relationship between trust and malware risk perception (i.e., for reducing malware perception) is stronger in the search engine than in the Amazon.com scenario. The reason for this difference could be that individuals exhibit more trust in Amazon.com. This means that the need for trust as a risk reduction mechanism is less in the Amazon.com scenario, than the need in the search engine scenario. We also found that the influence of computer risk propensity on click-through intention was significant in the Amazon scenario and was not in the search engine scenario. This result may indicate that an individual's risk propensity trait is a more important factor in the Amazon scenario (i.e., more trusted), more so than in the search engine scenario.

2.6.2 Contributions

This study contributes to IS research, trust in online transactions, and risky decision making literature. First, we proposed a theoretical model by adopting and combining both risky decision making and trust frameworks to identify factors that affect how Internet users form their decisions to click-through URL links in a risky environment. Trust has been used extensively in e-commerce research to explain "how" and "why" individuals engage in e-commerce transactions, but has not been used in understanding risky decision making in the information security context (click-through intention). We believe this is the first of many studies to research click-through intention in information security (i.e., Internet and malware) and e-commerce contexts. Second, our study answers the critical question of how trust affects security-based behavioral intentions from cybersecurity and e-commerce standpoint (Pfleeger and Caputo 2012). It does so by integrating trust in the risk framework and by applying the “where” aspects of theory building (Whetten, 1989). The hope is that this research advances information security context-related research, and increases the importance and specificity of trust, risk and security research.

In addition, we successfully demonstrate that the expansion of the risk framework to include trust and familiarity was valuable in explaining the model. We also show the influence of self-efficacy of information security in how individuals form click-through intention. The model was also tested under different scenarios, such as Amazon.com and search engine. We found interesting differences in some aspects of the relationship in each scenario. These differences confirm the notion that individuals may behave differently under different situations of risk.

Further, the findings portray the important role that risk propensity and risk perception play in risky decision making. The finding is a response to Keil et al. (2000), who argue for the development and relevance of computer risk propensity with respect to IS research. Our findings are also consistent with Chen et al. (2011), who find support for this relationship in an information security domain. Thus, confirming and highlighting the importance of risk propensity and risk perception to risky decision making.

The current study identifies malware risk severity as an important antecedent of malware risk perception. Thus, capturing the influence of problem environment in creating the model that explains risky decision making. The importance of risk severity in consumer behavior literature involving risks in online transactions has been established in prior literature (Grazioli and Jarvenpaa 2003). In addition, the findings provide evidence for the important role that trust and familiarity play in the risky decision making. Although prior literature has confirmed the importance of trust and familiarity in the presence of risks in e-commerce (e.g., Van Slyke et al. 2006), few studies have integrated trust in the risky decision making framework. Several studies (e.g., Featherman and Pavlou 2003; Pavlou 2003) found empirical support for the influence of trust and familiarity in online transactions that involve risks. The current study provides empirical evidence for the impact of trust and familiarity on Internet related risky decision making behavior. Thus, adding value to both risky decision making literature and trust in online transaction literature, and allowing for a comprehensive model that predicts risky decision making under risk and trust in an information security and e-commerce context. Lastly, we demonstrate that self-efficacy of information security influences one's click-through intention. Individuals who believe in their capability to identify malware websites and solve issues that arise as a result will tend to click-through URL links.

The current study also has a number of practical implications. Our findings indicate the significant impact of malware risk severity on risk perception. In order to continue the adoption and use of e-commerce and search engines for online transactions and information gathering respectively, the public needs to be aware of the severity of malware through campaigns and security, education, training and awareness (SETA) programs. Training is likely to enhance the skills individuals need to be able to detect and avoid threats in e-commerce and search engine environments. In addition, the results suggest that familiarity of the website significantly affects click-through intention. This indicates that individuals base their decision to click-through URL links on the extent that they are familiar with the website that they are currently on. Deception using fake websites and fake URLs is based on making the sites/URL (DELL 2015) look as familiar as the original. Hence, it is essential that practitioners and website owners train users on how to detect fake websites and URLs that look familiar. Cybercriminals have been known to use familiarity and trust cultivated from previous experiences to try to scam individuals (DELL 2015). Hence, it is a good idea for practitioners to post information that lists known cybercrime scams and fake websites/URLs that look like the practitioner sites/URLs. Doing so may increase click-through on sites, hence increasing revenues for organizations (e.g. search engines, social media advertisements) that depend on click-through for income.

2.6.3 Limitations and Future Directions

This paper is subject to several limitations that create opportunities for future research. First, as a scenario-based survey research, scenarios were presented to subjects about situations involving an Amazon.com and self-selected search. Future research can employ a lab experiment that requires subjects to complete tasks in similar environments (i.e., Amazon or search engine) and that manipulates trust and risk perception based on the environment. A lab experiment could also be used to evaluate the individual's intention to click-through after ignoring a browser's warning of the potentially harmful nature of the link. Second, another limitation is that we measured click-through intention in the context of only two scenarios. It is possible that click-through intention results will be different for scenarios describing other security or e-commerce situations.

Third, the data was based on university students. Though college students have experience using search engines for information gathering and have performed e-commerce transactions, future research can employ a more representative sample of users (e.g. professionals) in order to increase external validity. Furthermore, future research could include other determinants of malware risk perception to the study, such as previous malware experience, cultural differences, and malware susceptibility. In conclusion, by adopting and expanding risky decision making framework, this study identifies factors that form the individual’s intention to click-through Internet links.

ESSAY 3

TOP MANAGERS’ PERSPECTIVES ON CYBERINSURANCE RISK MANAGEMENT

3.1 Introduction

Despite global growth in security investments, security breaches continue to pervade the industry and are adversely affecting organizations’ finances (Cavusoglu et al. 2004; Mukhopadhyay et al. 2013). Ponemon (2015) notes that the average cost of each stolen record to an organization is $217. Recently, organizations face the theft or compromise of millions of records following each security breach incident (e.g. Verizon, Equifax, Yahoo!). The cost of data breaches, which includes notification of individuals impacted by the breach, legal fees, regulatory fines, and the post breach cost of recovery can be financially damaging to organizations. As a result, security risk management has gained more importance for not only minimizing vulnerability to breaches, but also for recovering from losses and reducing post breach costs.

Traditional approaches to security risk management in information systems (IS) literature mostly include three of the four methods: risk mitigation, risk acceptance, and risk avoidance, while risk transfer is least explored. These three approaches are aimed at deterrence, prevention, detection, and response (Straub and Welke 1998; Willison and Warkentin 2013). The approaches are implemented through *technology* such as intrusion detection systems and anti-virus software (e.g., Cavusoglu et al. 2005; Lee and Larsen 2009), security *policy* compliance and violation (e.g., Vance et al. 2012b) and *procedures* such as security training and awareness (D’Arcy et al. 2009; Posey et al. 2015). Scholars have argued that these approaches to security risks are rarely sufficient for providing an overall protection of IS assets (Herath and Rao 2009b; Ifinedo 2014; Vance et al. 2012a) or for reducing the cost of a security breach. Therefore, it is imperative that organizations consider integrating other risk management approaches for minimizing the likelihood of experiencing a successful cyber-attack and reducing the impact and cost of security breaches. Another dimension of security risk management that demands research emphasis is risk transfer through cyberinsurance. Researchers argue that an overall solution for cybersecurity must include cyberinsurance (Majuca et al. 2006; Siegel et al. 2002). Indeed, many government standards, financial, and regulatory initiatives encourage and sometimes demand the use cyberinsurance (e.g., NIST, Security and Exchange Commission, Department of Homeland Security, New York State Department of Financial Services etc.). For example, in 2011 the Security and Exchange Commission (SEC) announced that public firms disclose the type of insurance used in their cybersecurity plans (SEC 2011). In addition, New York State Department of Financial Services in 2014 expects banks to carry cyberinsurance policies (Lawsky 2014).

Cyberinsurance is defined as an insurance product used to protect organizations from risks derived from the use of the internet and information systems (Böhme and Kataria 2006). It is the transfer of financial risk associated with security/data breaches to a third party (Böhme and Schwartz 2010). Cyberinsurance is seen as a promising security risk management approach used for reducing the impact and severity of damage through financial means (Siegel et al. 2002). Cyberinsurance provides first-party and third-party coverage which enables organizations to transfer their security risks to an insurance company (Zhao et al. 2013). Even though cyberinsurance is relatively new, it is arguably the fastest growing niche insurance in the US (Meland et al. 2015). There are about 50 insurance companies offering cyberinsurance in the U.S. and the estimate for cyber insurance is about $2.5 billion. This market estimate is projected to grow to $7.5 billion in 2020 (Oltsik 2015).

Information security has traditionally been considered a domain for technology teams. However, as more organizations fall victim to cyber-attacks and suffer the consequences of customer churn, lost business, and reputation damage, business executives are beginning to pay more attention to security risks and its financial impact (Experian 2015). Coupled with the shifting of accountability in industry where top managers are under increased scrutiny for security breaches (Experian 2015), SEC currently requires organizations to disclose their risks of cyber-attacks, as well as the cost incurred to address cyber related issues. Because of their strong stakeholder responsibility and holistic influence on how organizations interpret and respond to events affecting their organizations' strategies (Kettinger et al. 2013), we are interested in examining the top manager's perspective. Specifically, this study is interested in understanding the top manager's commitment towards cyberinsurance as a risk management strategy. We seek to answer the research question: What are the salient factors that determine the top manager's commitment towards the use cyberinsurance as a risk management strategy?

Drawing from the valence framework, we propose a research model consisting of individual, organizational, and environmental risk factors. We postulate that top manager's commitment towards cyberinsurance is influenced by their job security, perception of breach risk, financial risk, transaction cost, regulation oversight risk, and cyberinsurance ambiguity. We test the model through a survey of 151 top managers from a diverse set of organizations. This study seeks to highlight the role of cyberinsurance as an information security risk management approach. Contributions to research include, theoretically identifying and outlining the factors that determine the top manager's commitment towards cyberinsurance in a nomological network. For practice, we hope the results of the research spur organizations to consider cyberinsurance as a security risk management strategy.

3.2 Literature Review

3.2.1 Security Breach Cost

Breaches have direct and indirect costs to organizations. In terms of direct costs, organizations are required to send notifications to affected individuals, which is expensive for most organizations. Researchers argue that the cost of notifying individuals is one of the main drivers for cyberinsurance (Marsh 2015). An indirect cost of sending notifications and disclosing the breach to the public has a potential for damaging to the firm's reputation and market value (Acquisti et al. 2006; Ponemon 2015a). Ponemon (2015a) notes that organizations could reduce the per-record cost of data breaches with the adoption of cyberinsurance. The per-record savings is about $4.40, which for a small business could be the difference between staying in business and closing shop. The size of small businesses limit their exposure to fewer breached records, and therefore fewer individuals to notify. Nevertheless, the overall cost can be devastating. Especially since 72 percent of security breaches occur at small and medium-sized businesses (Wall Street Journal 2012). Figures 3.1 and 3.2 depict the cost of security and data breaches. The figures reveal that healthcare industry has the highest per record costs, and that businesses suffer the most from lost business cost. The cost of data breaches include detection and escalation, post breach activities, notification, and lost business. Detection and escalation cost include forensics, assessment and audit activities. Notification cost include activities related to notification of individuals affected by the breach and fulfilling all regulatory requirements. Post breach cost include remediation activities, legal fees, customer service, and identity protection services. Although all of these costs seem to have reduced from 2008 to 2012, they are steadily increasing as of 2016, indicating that firms are investing heavily in these activities. Thus, firms may turn to cyberinsurance as a risk transfer strategy to help them defray the cost and stay in business.

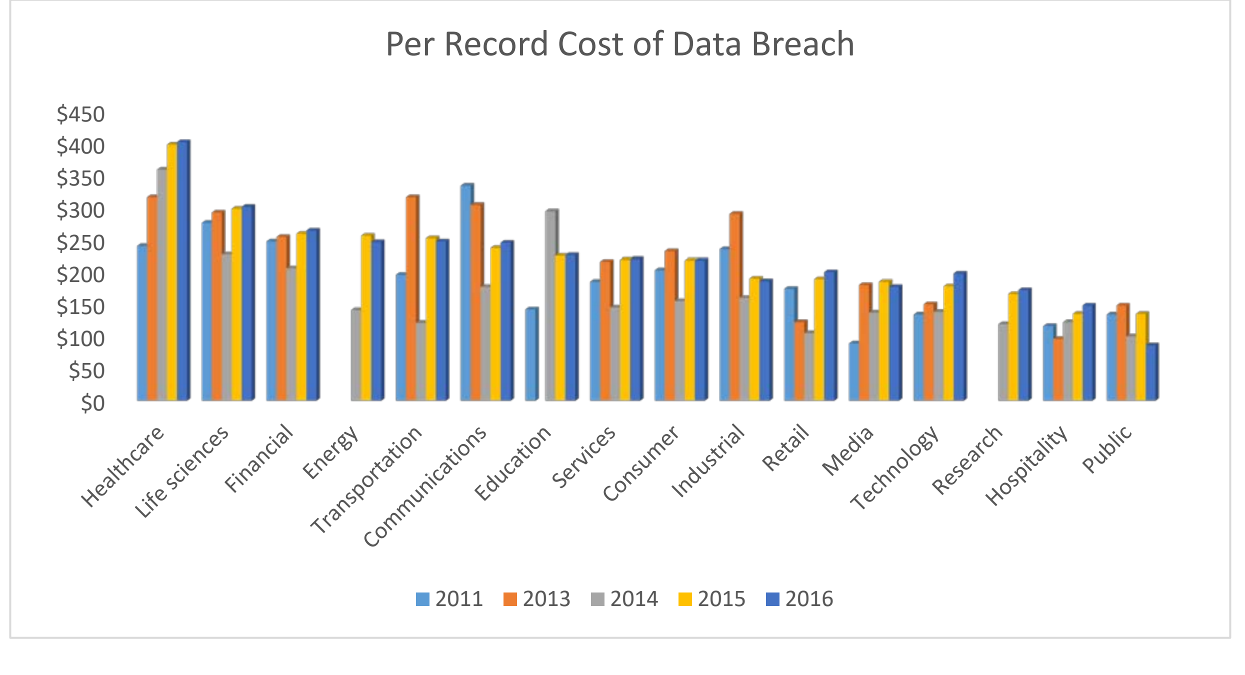

Figure 3.1: Per-Record Cost of Breach by Industry between 2011 and 2016 (Essay 3)
Note: 2012 data is not available (Ponemon 2015)

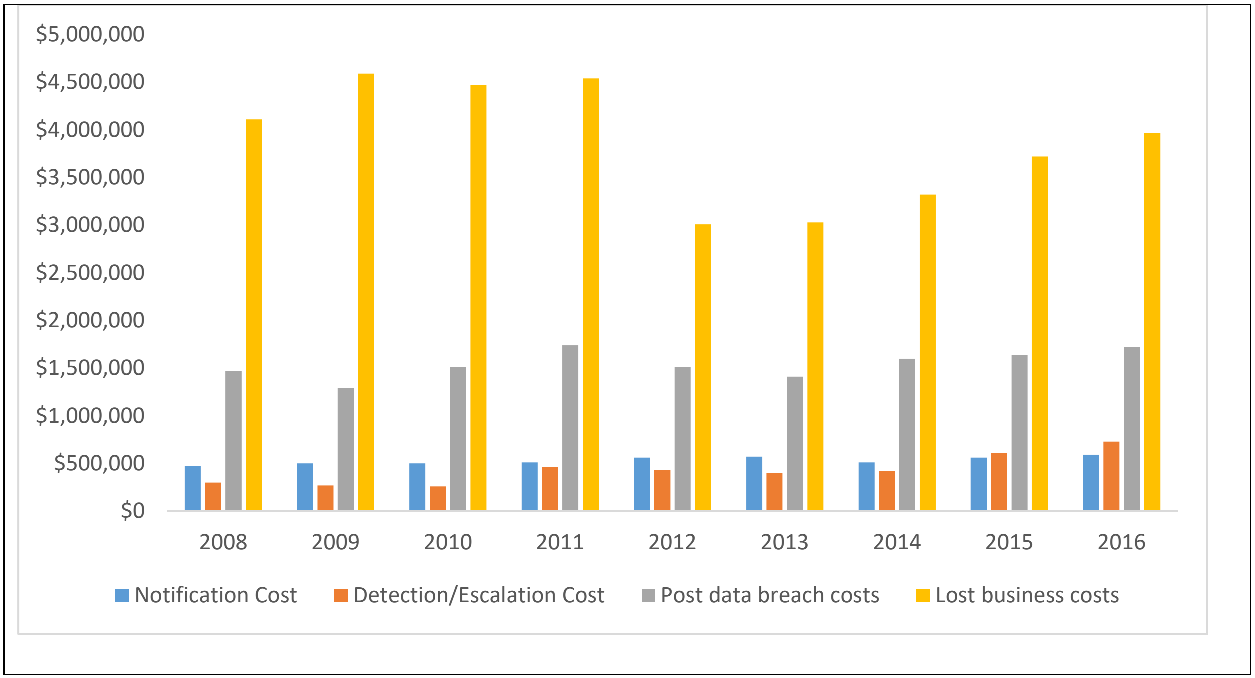

Figure 3.2: Average Cost of Breach by Year and Cost Item (Essay 3)
Note: Adapted from multiple years of Ponemon cost of data breach reports

3.2.2 Cyberinsurance Risk Management

The use of cyberinsurance in information security risk management dates back to Medvinsky et al. (1994) and Greer (2003) who proposed its use in the financial sector. Schneier (2001) introduced the topic in research by predicting that information security will be run by the insurance industry. Since then, a number of papers from both industry and research have proposed cyberinsurance as an effective risk management strategy. Gordon et al. (2003) compares cyberinsurance with other types of insurance products and notes the advantages of using cyberinsurance as a security risk management strategy. Supporting this notion, a demand-side explanation for why cyberinsurance is a cornerstone of security risk management programs is given (Bandyopadhyay et al. 2009). Mukhopadhyay et al. (2013) provides a decision model for effectively choosing a cyberinsurance product. Researchers have also used economic models to examine interdependent risks between firms, proposing cyberinsurance as a possible solution (Böhme and Schwartz 2010; Öğüt et al. 2011).

Zhao et al. (2013) examine risk pooling arrangements (RPA) and managed security services (MSS) as two alternative risk management approaches. They acknowledge the benefits of cyberinsurance as a complete risk transfer option used for reducing risk exposure and managing information security risks. In contrast with cyberinsurance, RPAs do not provide complete risk transfer and are primarily used in medical practices. MSSs provide complete risk transfer, however, only member firms are allowed to participate, which limits its availability to other firms. Also, regulatory restrictions in some jurisdictions do not allow mutual insurers like MSS/RPAs to carry certain types of insurance (Zhao et al. 2013). RPAs and MSSs are known to address interdependent risks that are inherent in security risks.

Organizations are taking a mixed approach to risk management by striking a balance between investing in security and accepting a level of loss (Meland et al. 2015). In addition to technical security, procedural security, and even self-insurance, organizations are purchasing cyberinsurance (Meland et al. 2015). In other words, risk transfer strategies such as cyberinsurance must be used in conjunction with other risk management options. In addition, cyberinsurance is increasingly being considered a method for incentivizing improved security decisions (Department of Homeland Security 2012; Naghizadeh and Liu 2016). The notion is that the requirements for obtaining cyberinsurance or enjoying continued coverage subjects organizations to security best practices such as encryption, backups, disaster recovery plans (Gordon et al. 2003; Young et al. 2016). Regulatory and government initiatives are calling for the adoption of cyberinsurance. For example, in its cybersecurity framework, NIST proposes that organizations manage their risks using all risk management strategies, including risk transfer (NIST 2013).

Even though the prevalence and severity of breaches have increased cyberinsurance awareness in industry, yet, only about one-third of businesses surveyed have adopted cyber insurance (Ponemon 2013). The numbers are smaller within small and medium sized organizations. A survey of small businesses revealed that even though 81 percent believe that cyberinsurance is a concern, only about 5 percent have adopted cyberinsurance (Experian 2016). In the UK, a report notes that only about 2 percent of large businesses in the U.K. have adopted cyberinsurance protection against damages related to a security and data breaches, while almost zero percent of small businesses have (Reuters 2015).

Cyberinsurance is a standalone product and not usually included in traditional insurance policies. Hence, most commercial insurance products exclude cyber related risks. Cyberinsurance includes first party and third party coverage. First party includes damages, loss, and cost associated with a breach incurred by the organization e.g. data loss, hacking, denial-of-service, theft of intellectual property, forensic investigation. Third-party coverage includes services or damages associated with others e.g., public relations, breach notifications to customers, legal expenses, credit monitoring, fines and penalties imposed by regulatory organizations or business partners.

3.2.3 The Top Manager

A firm with Jeff Bezos as a top manager may behave differently from one with Elon Musk as a top manager. Top managers are better able to have an overarching assessment of the impact of cyber-related risk throughout the organization. Goodhue and Straub (1991) argue that an organizations' security protective measures should require managerial careful attention. Studies (e.g., Bertrand and Schoar 2003) show that CEOs and other top level managers have an effect on their firms. Organizations consists of individuals that may account for the performance of organizations. Strategic management literature (e.g., Mollick 2012) suggest that the omission of individual factors in examining organizations has prevented a thorough understanding of the role individuals actually play in determining firm performance. It has been shown that top managers are considered to be important in determining firm performance (Bertrand and Schoar 2003; Hambrick et al. 1996; Mollick 2012). This literature have developed to explain risk-related behaviors at the individual and organizational levels. Specifically, the commitments of top managers are especially important because these executives have the authority necessary to influence actions in their firms (Finkelstein and Hambrick 1990; Weaver et al. 1999). For example, when matters of importance to firms such as firm performance and ethical standards are at stake, executive commitment towards such matters become imperative. SEC's recent requirements demonstrates the rising importance of security risk management to firms' financial wellbeing. In light of this, we seek to understand the top manager's commitment to cyberinsurance as a risk management strategy.

3.3 Theoretical Background

The valence framework is a motivational model derived primarily from the economics and organizational psychology literature (Goodwin 1996). The uniqueness of the expectancy-valence framework is that it relates a person's action to the perceived benefits and risks of the expected outcome (Feather 1988). It has been used in marketing, IS, and psychology to understand how the individual's simultaneous assessment of risk and benefit affect behavior (Peter and Tarpey 1975). A valence has been described as a "measure of the degree to which an individual values a particular reward", and involves the anticipated positive or negative affect associated with performing a certain action and experiencing outcomes. Transitioning from the motivational psychology of individuals to the behavior of top managers in corporations, we assume that the top manager's expectancies and valence will manifest in how they respond to issues in the organization. The expectancy–valence model has also been used as a behavioral framework to study individual's motivation and performance in an organizational context (Kren 1990). Expectancy has been shown to be a function of individual factors, situational factors such as perceived environmental uncertainty, and organizational factors (Desanctis 1982). The challenge, therefore for this study is to determine which variables are relevant for the commitment towards cyberinsurance as a risk management strategy.

The valence refers to the agent's utility function. In terms of the individual factors, the similarities between the agency theory and expectancy theory is perhaps why the economics and management literature usually used them together in behavioral models (Sloof and van Praag

2008). Using the valence framework (expectancy-valence) of risk and benefits perspective, we first identify factors and then model the relationship between the identified factors and the top manager's commitment towards cyberinsurance as a risk management strategy. We seek to extend the valence framework, by examining dimensions of risk and benefit factors along the lines of situational relevant factors and product relevant factors. Furthermore, we categorize risks and benefits based on their relevance to the individual, organizational and environmental factors. The notion is that the examination of risks and benefits based on their relevance may further increase our understanding of how they influence the top manager's decision-making (Lazarus and Smith 1988). Table 3.1 depicts a categorization of each factor, its description, relevance to the current study, and references. The individual factor refers to whether the top manager's cyberinsurance decision is relevant to his/her personal well-being.

Organizational factor refers to the top manager's interpretations of the organizational risks that the organization stands to incur. We identify risks such as financial risk (situational risk) and transaction cost (product risk). Environmental factor refers to factors outside the individual's or organization's control that affect their decision making (Lazarus and Smith 1988). We identify regulation (situational risk) and cyberinsurance ambiguity (product risk). Figure 3.3 shows the research model.

Table 3.1: Categorization by Individual, Organizational, and Environmental Factors (Essay

Category	Description	Relevance	Dimensions	Factors and their references
Individual	Refers to whether a decision is relevant to a person’s well-being or will affect the individual in any way (Lazarus and Smith 1988).	1. What personal factors affect one’s commitment towards cyberinsurance?	Situational benefit	• Job security (Adams et al. 2011; Hsu et al. 2003; McKnight et al. 2009; Moore 2000) • Manager’s tenure and experience (Adams et al. 2011)
		2. How does the manager’s personal perception of risk affect their committing to cyberinsurance?	Situational risk	Breach risk perception (Herath and Rao 2009b; Sen and Borle 2015; Straub and Welke 1998)
Organizational	Organizational sources of executive sense-making (Plambeck and Weber 2010)	What organizational factors affect the commitment towards cyberinsurance?	Situational risk	Financial risk and economic loss (Srinidhi et al. 2015)
			Product risk	Transaction cost (Ang and Straub 1998; Benaroch and Fink 2016)
Environmental	Refers to whether there are factors outside the individual’s or organization’s control that affect their decision making (Lazarus and Smith 1988)	How do environmental factors affect commitment towards cyberinsurance?	Situational risk	*Regulation* (Dinev et al. 2012; Miltgen and Smith 2015; Sen and Borle 2015)
			Product risk	*Ambiguity* (Carson et al. 2006)

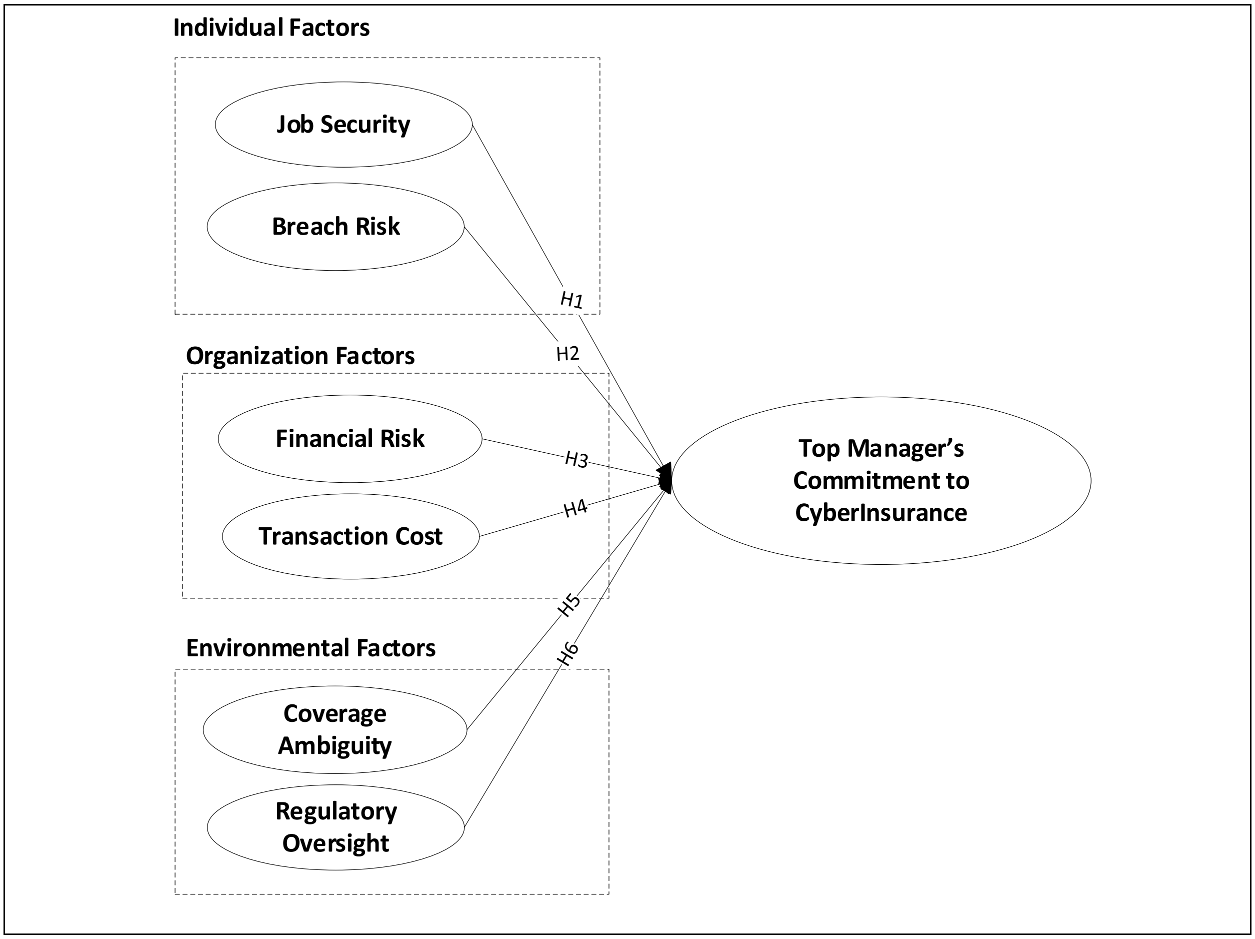

Figure 3.3: Research Model (Essay 3)

3.4 Hypotheses

3.4.1 Individual Factors

Personal meaning is a primary appraisal process that addresses how and whether a decision is relevant to a person's well-being (Lazarus and Smith 1988) or whether it will affect the individual in any way. In other words, it addresses whether an individual has a personal stake in the matter at hand. The effect of personal relevance on motivation and judgement has been extensively studied in the literature (e.g., Ajzen and Brown 1996; Cacioppo et al. 1996). The notion is that when individuals identify the relevance of the decision to their person, they assess the impact of their decision and would more likely make a decision that protects their interest (Albarracín and

Kumkale 2003). Because individuals are exposed to many stimuli, it would be very difficult to really think about all of them. Hence, individuals will pay close attention to only decisions with high relevance and consequence (Cacioppo et al. 1996). According to the agency view, the interest of individuals and their organization is not always aligned. An individual could have future political ambitions and therefore want to avoid any form of personal litigation. A top manager, whose interest is to avoid any litigation, may perform necessary activities that limits the organizations exposure. The top manager's decision is dictated by the relevance of the consequences of the decision to the manager. That is, if s/he makes the decision to forgo cyberinsurance, and a hacking event occurs, how will this affect the top manager's personal life, job, reputation, ambitions? Hence, the personal relevance factor asks the question: how does committing to cyberinsurance affect me personally? The answer to this question depends on factors most important to the decision maker. One such factor job security.

Top managers may be motivated to engage in risk management if it enhances their job security or performance (Adams et al. 2011; Doherty 2000). The manager's ability to tolerate risk or engage in actions to manage risk is affected by their perceptions of job security (Kwak and LaPlace 2005). If a top manager believes that engaging in risk management activities will provide job security, the likelihood increases that s/he will engage. The impact of security breaches on the organization (e.g. loss of revenue, reputation damage, and financial loss) can cause major organizational changes that affect the top manager. Organizations have been known to demote or fire top managers for security breaches. For example, Target was advised to sever ties with 7 out of 10 directors for not managing Target's systems to the best of their ability (Ziobro and Lublin 2014). In 2014, Target CEO, Gregg Steinhafel resigned from all his position. Home Depot's CEO Frank Blake announced his retirement as CEO shortly before the September 2014 breach. Amy

Pascal, former CEO of Sony, was also fired as a direct result of the 2014 security breach (CSO 2016). The agency-theoretic view suggests that managers are interested in investments that can protect the firm's assets and therefore, protect their job and pay (Srinidhi et al. 2015). Hence, in order to have job security, the top manager may support risk management strategies that enhance his/her job security. Studies have found a relationship between one perception of job security/insecurity and their commitment to a course of action (Fox and Staw 1979). Moreover, a recent survey shows that many (58%) IT decision-makers believe they will lose their jobs due to a security breach (Absolute 2015). Job security is an internal and individual anchor and has been linked to long-term employment and financial security. Job security has been researched in IS as a determinant to behavioral intention to leave (Hsu et al. 2003; McKnight et al. 2009). Therefore, we hypothesize:

> H1: Job security is positively related to the top manager's commitment towards using cyberinsurance as a risk management strategy

Risk exposure and loss experience are important drivers that may affect the manager's commitment towards cyberinsurance. Prior studies on insurance decisions include the determination of individual's risk preference in the decision for insurance. Security breaches and their impact on organizations have motivated many studies in IS research. Prior studies have found that data breach events have a negative effect on firm's market value and performance (Bose and Leung 2014; Goel and Shawky 2014; Gordon et al. 2011; Wang et al. 2013). The disclosure of security breaches resulted in 2.1 (Cavusoglu et al. 2004), 1.9 (Campbell et al. 2003), 0.58 (Acquisti et al. 2006) and 0.65 (Wattal and Telang 2004) percent loss of organizations' market value within a few days of announcement. A top manager's perception of the severity of a security breach will seek strategies that help his/her organization recover from such an event.

> H2: Breach risk severity is positively related to the top manager's commitment towards using cyberinsurance as a risk management strategy

3.4.2 Organizational Factors

McKinsey estimates that by 2020, the economic losses due to cyberattacks will reach $3 trillion Financial losses due to cyberattacks can lead to the closure of the business (Newman and Stein 2013). Security breach is a major challenge to organizations, which must grapple with consequences that include reputation loss, financial loss and corporate liability (Bulgurcu et al. 2010). Deloitte (2014) identified information security issues in the top three issues affecting organizations. It is expected that organizations and their top managers will attempt to signal to their stakeholders their concern about cybersecurity risk management approaches taken to address the issue. Cyberinsurance is one important mechanism through which organizations can signal cybersecurity performance to stakeholders (e.g., consumers, investors, shareholders). Regulators and shareholders are concerned about the financial and economic loss that organizations incur as a result of cyberattacks. Indeed, the SEC currently requires organizations to disclose their risks of cybercrime, as well as the cost incurred to address cyber related issues. Given that cybersecurity is seen as an important element of organization financial risk (Srinidhi et al. 2015), it is important to understand how the perception of financial risk affects risk management decision making. We define financial risk as the individual's assessment of the potential for financial loss associated with security breaches. Because organizations face financial risks including penalties for compromised data, costs incur to cover post breach activities, and lost revenue, top managers in organization may look for strategies to help their organizations cover these costs. Insurance decisions are typically decisions about financial risk. Cyberinsurance is known to cover these costs. Hence, we expect that top managers will commit to using cyberinsurance as a risk management strategy. Therefore, we hypothesize:

H3: Financial risk perception is positively related to the top manager's commitment towards using cyberinsurance as a risk management strategy

Transaction costs are related to the effort, time, and costs associated with searching, knowledge transfer, creating, negotiating, monitoring, and enforcing a contract between a client and vendor (Benaroch and Fink 2016; Dhar and Balakrishnan 2006). Since cyberinsurance like other insurance products is a contract, transaction cost is considered a determinant of the top manager's commitment toward cyberinsurance. Prior research considers transaction cost in the design of contracts (Benaroch and Fink 2016) for outsourcing (Ang and Straub 1998). Both ex ante transaction costs (e.g. negotiating) and ex post transaction costs (e.g. haggling) are combined to examine whether transaction cost affects cyberinsurance commitment decision. Inspired by transaction cost theory we examine the individual's perception of the extra cost that their organization incurs in their commitment towards cyberinsurance. The ex-ante transaction cost starts at the pre-contract and contracting stages where the objective is for the parties to develop a general understanding of the requirements. These costs are searching, knowledge transfer (Benaroch and Fink 2016), and negotiating costs. It takes considerable time and effort to identify the insurance vendor, transfer and integrate knowledge between the organization and insurance provider, and negotiate the contract. Researchers note the significant challenge in integrating the different knowledge types (Tiwana 2003) during knowledge transfer (Benaroch and Fink 2016), drafting and negotiating a contract (Dibbern et al. 2008). Specifically, each of these processes involves both parties spending time with each other to understand and develop requirements for the target insurance product. Hence, we expect that costs related to searching for the appropriate insurance product, transferring knowledge transfer between parties, and negotiating the contract will influence top manager's commitment toward cyberinsurance. Therefore, we hypothesize:

> H4: Transaction cost is negatively related to the top manager's commitment towards using cyberinsurance as a risk management strategy

3.4.3 Environmental Factors

Lazarus and Smith (1988) argue that even though an important aspect of appraisal is personal relevance of a decision to the individual, there is also the importance of the relationship between the person and the environment. This concept postulates that personal meaning is meaningful only when considered in reference to the person and their environment. In other words, the appraisal must reconcile one's personal goals with those of the organization or environment affecting the decision (e.g., regulation, laws, market conditions).Well-being is threatened when appraisal fails to consider the environmental requirements (Lazarus and Smith 1988). We examine here two aspects of environmental factors that prior research indicates may be relevant to decision-making: regulatory oversight and ambiguity.

The main purpose of regulatory oversight is to ensure that those to whom authority is delegated remain responsive (Ogul and Rockman 1990). Regulatory oversight can be used to correct market failures such as health safety and environmental risks (Collins and Urban 2014). An entity for regulation oversight is usually a centralized government agency that has the expertise to supervise regulated actions by organizations (Collins and Urban 2014). Hence, we define regulatory oversight as the degree to which a government body supervises and oversees firm's regulated actions. Previous research describes it as regulatory expectations, which is the notion is that regulators can decree certain rules that guide the relationship between merchants and their customers (Dinev et al. 2012). Where enforcement seems to deter violations and increases the likelihood of fines and a cycle of negative publicity (Collins and Urban 2014).

The prevalence of cyber-attacks and security breaches gave rise to legislation that mandated breach disclosure in the healthcare sector (Kwon and Johnson 2014). The law requires businesses to disclose breaches involving individuals. The Department of Health and Human

Services and the Federal Trade Commission (FTC) are two main regulatory organizations tasked with issuing breach notification rules that apply to healthcare entities and the business associates, health information systems vendors, and other entities that provide non health related services (Kierkegaard 2012). Organizations subject to regulatory oversight tend to be more vigilant in the monitoring of internal controls (Boo and Sharma 2008). Not surprising, researchers suggest that mandated data breach disclosure laws increase the perception of data breach risk within heavily regulated industries such as financial, educational, and healthcare (Sen and Borle 2015). Because legislation for breach notification have prompted security investments (Kwon and Johnson 2014) and the transfer of notification costs to third parties via cyberinsurance (Marsh 2015), we expect that regulatory oversight will affect the top manager's commitment towards cyberinsurance. Therefore, we hypothesize:

> H6: Regulatory oversight is positively related to the top manager's commitment towards using cyberinsurance as a risk management strategy

Ambiguity has been defined as the degree of uncertainty in the perceptions of the environmental state irrespective of its change over time (Carson et al. 2006). Ambiguity also refers to the "lack of clarity about the meaning and implications of particular events or situations" (Santos and Eisenhardt 2009, p. 644). Ambiguity is usually experienced in environments characterized by "novelty, complexity, or insolubility" (Budner, 1962, p. 30). Following Carson et al. 2006, we define cyberinsurance market ambiguity as the degree of uncertainty inherent in perceptions of the environmental state of the cyberinsurance market. Ambiguity includes several aspects, such as lack of information clarity, uncertainty related to the importance of environmental variables, and uncertainty about the next course of action and their possible impact (Daft and Macintosh 1981). Researchers have often referred to ambiguity as equivocality. Equivocality means a state of confusion, disagreements and lack of understanding, where managers may be uncertain about the questions to ask (Daft et al. 1987). In terms of cyberinsurance market, top managers may be uncertain about the policies and the types of coverages. Especially since the cyberinsurance market is not yet mature and there is insufficient actuarial data available for insurers to properly insure against all losses (Naghizadeh and Liu 2016). Even though cyberinsurance policies are meant to close the gap, they lack standardized forms, content, and vocabulary (Meland et al. 2015). Researchers argue that the emergence of new technologies and markets increase the possibility that organizations will face ambiguous environments (Petkova et al. 2014; Santos and Eisenhardt 2009). In other words, as newer technologies emerge and the risks they create evolve, the chances that organizations will face ambiguity in cyberinsurance coverage policies also increases. Hence, understanding the role of ambiguity in the top manager's commitment to adopt cyberinsurance is therefore of theoretical importance. We propose ambiguity as a barrier confronting commitment towards cyberinsurance. Therefore, we hypothesize:

> H7: Cyberinsurance coverage ambiguity is negatively related to the top manager's commitment towards using cyberinsurance as a risk management strategy

3.5 Methodology

3.5.1 Measures

3.5.1.1 Dependent Variable

Commitment to cyberinsurance as a risk management strategy is measured by asking participants to indicate the extent of their agreement to the questions. We measured top manager's commitment by adapting four items from Lewis et al. (2003). We changed the wording of the scales to reflect the top manager's attitudes toward a strategic decision and not attitudes toward their organization. Thus, the adapted scales measured the extent to which the top manager is committed to the use of cyberinsurance to manage security risks in his/her organization. These included questions about the commitment to a vision of adopting cyberinsurance, commitment to supporting efforts and resources for its adoption, commitment to encouraging the use of cyberinsurance for managing security risks, and the recognition of the importance of using cyberinsurance for managing security risks. The following sections include the independent variables and control variables used in the study.

3.5.1.2 Independent Variables

Though we made considerable effort to use previously validated measures, some of the constructs required new items that capture the content, context, and domain of the study. Hence, we systematically developed measures following the procedure suggested by Moore and Benbasat (1991). The instrument development is depicted in Appendix C1. We paid close attention to content validity of the instruments as we conducted a Q-Sort and a pretest of the survey instruments to ensure that constructs in cyberinsurance domains are covered by their items. *Regulatory oversight* is a new construct that assesses the extent to which a government agency has regulatory oversight over the organization's activities. The items measure whether a government agency specifies objectives and criteria that govern the organizations operations (e.g. breach notifications), works with the organization to remedy and conform to regulatory actions, and can revoke licenses or certifications to continue to provide services. The measures are constructed from regulatory provisions from the Office of National Coordinator for Health Information Technology and National Transportation Safety Board, which have regulatory oversight for health information and transportation regulation, respectively. Though we adapted measures from Ashford et al. (1989) and McKnight et al. (2009) for *job security*, new measures were also developed. The measures include items measuring the top manager's perception of whether cyberinsurance will protect 'my' job, offer me continued long-term job security, control the undesirable events that might affect my job, and reduce negative events from affecting my job. *Breach risk* is measured by items adapted from Milne and Orbell (2000) that assess the degree to which the top manager believes that the consequences of the security breach would be severe to their organization. Hence, measures cover the domain of security breach consequences such as expenses to recover from and cover the cost of breach, disruption to business operations and customer loss. *Financial risk* measures the potential for financial loss associated with security breaches including notification costs, fines, lost revenue, reporting requirements. Measures are adapted from Featherman and Pavlou (2003) and Ponemon's cost of data breach (2015b). *Transaction cost* is measured by items adapted from Jones et al. (2000) and transaction cost content (e.g. Choudhury and Sampler 1997) that covers the contracting and coordination costs of cyberinsurance related to the effort, time, and costs associated with searching, knowledge transfer, creating, negotiating, monitoring, and enforcing a cyberinsurance contract between the top manager's organization and an insurance vendor. *Cyberinsurance ambiguity* measures the degree of uncertainty inherent in perceptions of the state of cyberinsurance market. Its measures are adapted from Carson et al. (2006) and captures the difficulty understanding the risks covered by cyberinsurance, the lack of common language in the meaning of cyber incidents covered, lack of clarity about the limits of coverage policies, and lack of clarity about the adaptation of cyberinsurance to technological changes.

3.5.1.3 Control Variables

Control variables in this study are prior knowledge of cyberinsurance, organizational tenure,_industry, organization size (number of employees, revenue), experience in information security management, and experience in technology management. Organization tenure is suggested to have an effect on outcomes and commitment (Finkelstein and Hambrick 1990). Prior studies have used similar control variables, such as organization size, and type (Kankanhalli et al. 2003; Weaver et al. 1999) to examine management commitment and support. Top management commitment to security risk may differ based on whether their organization is regulated (e.g. healthcare and finance) (see Sen and Borle 2015). All control variables in the model are single item measures.

3.5.2 Instrument Development

The survey instrument was pretested with university students who were asked to comment on the questions, to raise concerns related to the questionnaire, and to describe any ambiguities. To address the concerns of content validity, earlier versions of the questionnaire were also pretested with five professionals familiar with cybersecurity risk and cyberinsurance. The survey questions were then modified according to the comments from researchers and professionals. The constructs are operationalized and adapted from established literature. The constructs are measured using seven-point Likert ranging from "strongly agree" to "strongly disagree", differential semantics, and open-ended questions.

3.5.3 Data Collection

To test our model and hypotheses within the cyber risk management context, a cross-sectional survey is administered to top managers in organizations to determine the predictors of commitment towards cyberinsurance as a risk management strategy. Top managers in organizations were targeted for answering our survey because we framed our research to understand the factors that facilitate their commitment to cyberinsurance. Specifically, the selected respondents were executive-level managers and the ones who are most likely to be aware of the strategic positioning of cyberinsurance to their organization. This follows the key informant approach, where the individual within the organization who is most knowledgeable about the aspects of the topic is selected (Sabherwal and Chan 2001, Wall et al. 2004). Moreover, as security risks ascend in its level of importance to organizations (Kappelman et al. 2017), top managers of firms are increasingly expected to understand the management of such risks (Experian 2014). Only participants who indicated that they make insurance purchase decisions were included in the data analysis. The population of interest includes top-level directors or officers such as the Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, or an individual designated as a risk manager. Participants were recruited through a Qualtrics Panels, a service that attempts to match researchers in need of samples with individuals willing to complete surveys. It has a database of voluntarily registered survey participants. Empirical studies using data collected from Qualtrics have appeared in IS journals (e.g. Wang et al. 2017; Warkentin et al. 2017). We solicited 151 respondents to participate via a paid Qualtrics panel of CEOs in the United States. To decrease respondent concerns about social desirability and reporting their behavior, respondents were told: "there are no right or wrong answers, please answer questions as honestly as possible. Further, all responses are anonymous, will be aggregated, analyzed and reported without linking them to any single company or individual."

Table 3.2: Profile of Respondents (Essay 3)

	Category	Percent
Industry	Manufacturing	8.6
	Banking	2.6
	Finance	5.3
	Insurance	2.0
	Retail	12.6
	Transportation	1.3
		(table continues)

	Category	Percent
	Education	2.6
	Technology	17.2
	Health	4.6
	Government	1.3
	Services	31.1
	Other	10.6
	Total	*100.0*
Employees	10,000 or more	2.6
	5,000 - 9,999	9.3
	1,500 - 4,499	4.6
	500 - 1,499	10.6
	100 - 449	21.2
	50 - 99	12.6
	10 to 49	39.1
	Total	*100.0*
Revenue (U.S. Dollars)	$5 Billion or More	2.0
	$1 Billion – Under $5 Billion	8.6
	$250 Million – Under $1 Billion	4.6
	$100 Million – Under $250 Million	4.0
	$50 Million – Under $100 Million	6.0
	$15 Million – Under $50 Million	4.0
	$10 Million – Under $15 Million	7.3
	$5 Million – Under $10 Million	13.2
	$1 Million – Under $5 Million	31.8
	Under $1 Million	18.5
	Total	*100.0*
Adopted Cyberinsurance	Yes	51
	No	49
	Total	*100.0*
Previous Cyberinsurance Knowledge	Yes	84.1
	No	15.9
	Total	*100.0*

The survey respondents represent a broad sample in regards to the industry, employee size, and annual revenue (Table 3.2). 31% of the respondents indicated services as their industry, and 17% indicated technology, while the rest belong to various areas. Respondents that indicated other specified tourism, nonprofit, music, agriculture, athletics, wholesale, as their industries. All the respondents are presidents and owners of their respective firms. 84% had knowledge of cyberinsurance prior to the survey, and 51% have adopted cyberinsurance.

3.6 Results

In analyzing the theoretical model, we used partial least squares (PLS) using SmartPLS 2.0 (Ringle et al. 2005). We chose PLS rather than a covariance-based SEM technique such as AMOS because PLS is considered to be better suited than factor-based covariance fitting approaches when the primary goal is to predict, rather than to test established theory (Chin et al. 2003; Gefen et al. 2005). Furthermore, PLS is appropriate for exploratory research (Hair Jr et al. 2016), which is suitable for the exploratory nature of this study.

3.6.1 Measurement Model Testing

We document the tests performed to validate our model in Appendix B2, which includes tests for convergent and discriminant validity and common method bias. The results of these tests demonstrate that our model meets or exceeds the rigorous standards expected in IS research (Straub et al. 2004). Since the measurement model demonstrated adequate validity, the structural model was evaluated next.

3.6.2 Structural Model Results

In testing our structural model, we used 4,999 (Henseler et al. 2016) bootstrap iterations for significance testing. Specially, we used bias corrected bootstrap confidence interval. Control variables are examined prior to evaluating the model hypotheses. Only general experience is significant in its relationship to COMM, indicating that top managers' years of experience in technology management may influence their COMM. The other control variables - revenue, employee, industry, knew, tenure - were irrelevant to COMM. All the constructs in the structural model is analyzed as reflective constructs. The results of the analysis for the hypothesized relationships including the standardized regression weights and level of significance can be found in Table 3.3; Figure 3.4 provides the final model paths. The R^2 value for COMM is 0.69 and adjusted R^2 is 0.678.

Individual, organizational, and environmental factors are associated with commitment towards cyberinsurance as a risk management strategy. We find statistically significant relations between JSEC and COMM (p <0.001), supporting H1. The individual factor of security breach SEV and COMM (p < 0.01) is significant, supporting H2. The organization risk factor FIN is significant in its relationship with COMM (p < 0.05), supporting H3. The organizational factor, TXNC is significantly associated with COMM (p < 0.05), supporting H4. We find that the environmental factor AMB is not significantly associated with COMM. Thus, H5 is not supported. Finally, there is a significant relationship between REG and COMM (p < 0.05). This supports H46. For the relationships that are significant, we assess their effect sizes. It appears that the effect sizes for FIN, JSEC, REG, SEV and TXNC are 0.052 0.316, 0.042, 0.069, and 0.114 respectively. Overall, job security has a medium high effect size (f^2 = 0.316) followed by transaction cost (f^2 = 0.114) and they appear to be more important than the other effects.

Table 3.3: Path Analysis Results (Essay 3)

	Path Coef	f^2	STDEV	T-Stat	P-Values	CI 2.50%	CI 97.50%	Result
JSEC → COMM	0.438	0.316	0.082	5.315	0.000	0.258	0.584	Accept
SEV → COMM	0.214	0.069	0.080	2.680	0.007	0.062	0.372	Accept
FIN → COMM	0.177	0.052	0.080	2.211	0.027	0.025	0.341	Accept
TXNC → COMM	-0.226	0.114	0.092	2.455	0.014	-0.365	-0.079	Accept
AMB → COMM	0.08	0.014	0.071	1.128	0.260	-0.041	0.226	Reject
REG → COMM	0.141	0.042	0.066	2.141	0.032	0.019	0.276	Accept

Table Legend: COMM = Commitment towards using Cyberinsurance as a Risk Management Strategy; AMBG = Ambiguity of Cyberinsurance; FIN= Financial Risk; REG = Regulation Oversight Risk; TXNCN = Transaction Cost; SEV = Breach Risk Severity; JSEC = Job Security

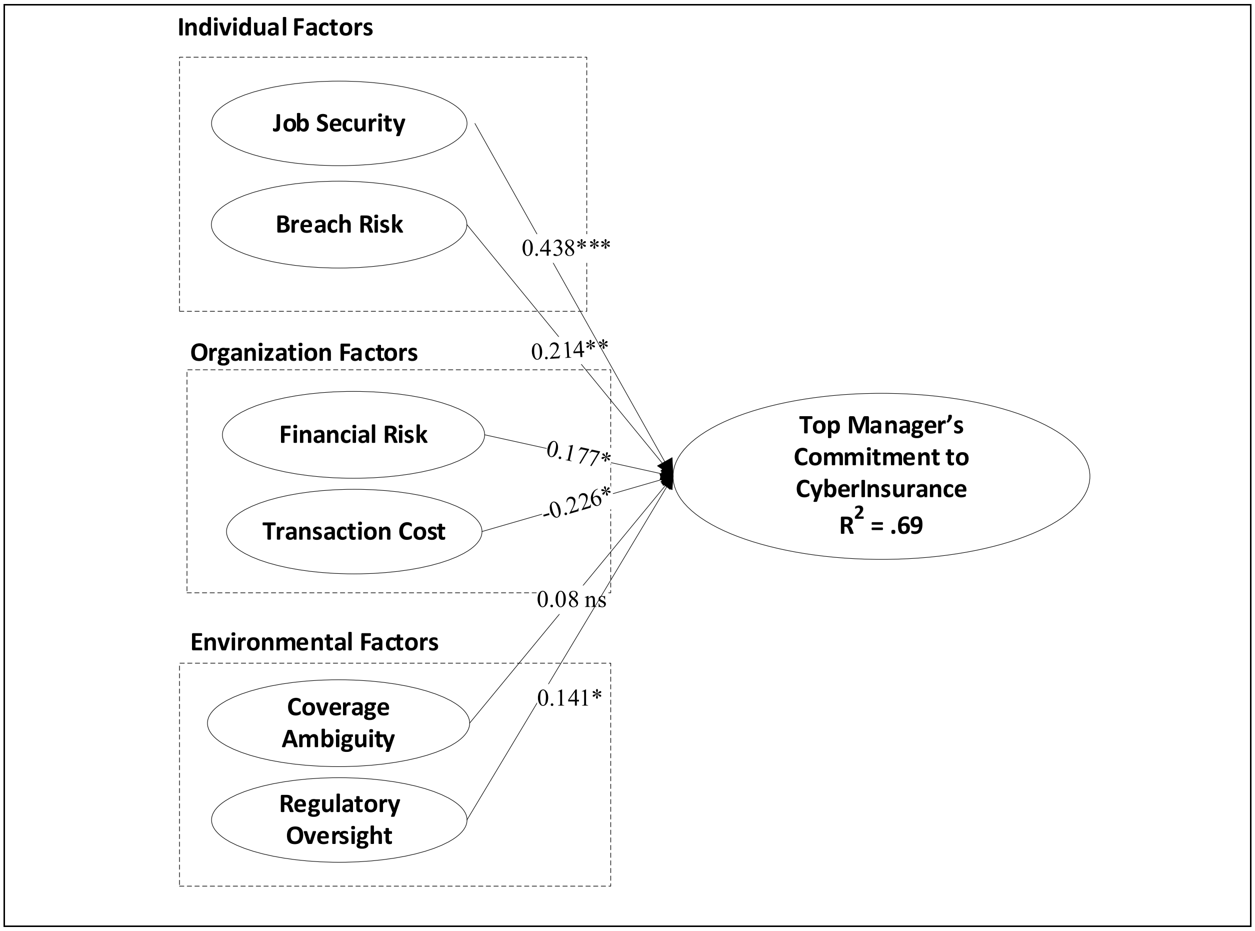

Figure 3.4: Structural Model Paths

3.7 Discussion

Due to increased impact of security breaches to organizations' financial well-being, top managers are increasingly held accountable for their organization's security risk management. Security risk management has traditionally involved using technology, processes, and procedures to deter, prevent, detect, and respond to security issues. However, technology, processes, and procedures are not enough to help organizations deal with or recover from the effects of a breach. Moreover, these methods fall into only three of the four aspects of risk management: risk mitigation, risk avoidance, and risk acceptance. The fourth aspect, risk transfer has received little attention in IS research. Hence, we explore the risk transfer aspect of risk management through cyberinsurance. Specifically, we investigate it through the lens of the top manager. We seek to understand the top manager's commitment towards cyberinsurance as a risk management strategy. We drew on the valence framework and argued that individual factors (i.e., job security and perception of breach risk severity), organizational factors (i.e., financial risk and transaction cost), and environmental factors (i.e., regulation oversight risk and ambiguity of cyberinsurance) will predict the top manager's commitment towards using cyberinsurance as a risk management strategy. Our results confirm most of our predictions, and underscore the importance and the consideration of individual, organizational, and environmental factors in driving one's commitment towards cyberinsurance. Individual factors of job security was more strongly associated with top manager's commitment towards cyberinsurance than were organizational and environmental influencers.

3.7.1 Theoretical Implications

This study contributes to information security research. The work expands the valence framework of benefits and risk and their influence on one’s decision, by examining dimensions of risk and benefit factors along the lines of situational factors and product factors. Such an approach explores the deeper aspects of the decision element under consideration, complements and extends traditional views related to decision making through valence framework lens. Whereas, traditional views broadly explore benefits and risks of an element under consideration, this study goes a step further by delineating and examined risks and benefits in terms of their situational and product factors. In addition, we incorporate risk and benefit factors with relevance to the top manager (individual), their interpretation of organization’s risks (organization), and their interpretation of factors outside the individual’s or organization’s control (environment). We believe that this type of extended view provides a more comprehensive insight and evidence of the decision-making process. The model presented in this study complements and extends prior valence framework research in two ways: (1) explicitly delineates risk and benefits of top manager’s commitment to cyberinsurance based on situational and product aspects, and (2) goes beyond traditional conceptualizations of benefit and risks considerations in decision making, and examines the personal, organizational, and environmental relevance. Our work complements research that has focused on other decision outcomes such as purchase intention using a similar framework (e.g., Kim et al. 2009) and extends work that focuses on other approaches to security risk management (e.g., Zhao et al. 2013).

Interestingly, the results of this study in terms of the individual, organizational and environmental factors have contributions and implications for IS research. The individual factor, job security significantly facilitates the top manager’s commitment towards cyberinsurance. In other words, the interest of the top manager to keep his/her job has the greatest impact on whether they commit to this risk management strategy. In terms of agency theory and expectancy theory, managers are interested in investments that can protect the firm's assets and therefore, protect their job and pay (Srinidhi et al. 2015). This result suggests that when considering a risk management strategy, top managers may be more concerned about its relevance to their continuation in their current position, more so than other factors. This work offers new boundary for information security research, highlighting the fact that just as personal relevance is important in employees' motivation in pursue adaptive secure behaviors, it is pronounced in their manager's commitment to the risk management approach that makes such secure behaviors possible in the first place. Thus, underlining the importance of understanding how and why organization leaders decide on which risk management approaches are use in their organizations.

Information security research has often focused on technologies, processes, and procedures that deter, prevent, detect, and respond to security issues (e.g., Cavusoglu et al. 2005; Straub and Welke 1998; Vance et al. 2012b; Willison and Warkentin 2013). Much of this research has either treated information security from an employee behavior perspective (e.g., policy compliance and violation) or focused on few risk management approaches (e.g., risk mitigation), which does not provide an overall solution. By examining the risk transfer aspect of security risk management using cyberinsurance, this study adds to the literature that focuses on security risk transfer strategies (e.g., pooling hedging, insurance).

We examined security based decision making in terms of the top manager's commitment (i.e., decision making), which is different from the employee's security decision making perspective. Top managers' commitments are important because they have the authority necessary to influence actions in the organization (Finkelstein and Hambrick 1990; Weaver et al. 1999). Indeed, the top manager's commitment influences the choice of risk management strategies or security application that their organizations implement. Hence, not only do we add to the literature on top manager’s decision making in information security domain (e.g., Lee and Larsen 2009), we also extend this literature by doing so in terms of a risk transfer strategy.

3.7.2 Practical Implications

Our results indicate that individual factors such as job security is most strongly linked to top manager’s commitment to cyberinsurance as a risk management strategy, rather than environmental and organizational influences. Shareholders that leverage this result to incentivize their organizations’ leadership towards security risk management might be more successful if more attention is paid to job security rather than organizational and environmental risk factors. Financial reporting requirements such as Securities and Exchange Commission requirement for disclosing cybersecurity risks and incidents, provide a strong incentive for firms to develop comprehensive security risk management strategies that include all dimensions (acceptance, mitigation, avoidance and transference) programs, so that should they get breached, they can say that they did all of the "right" things.

The volatility of cyber risks and threats pose challenges to the adoption of cyberinsurance. This creates a problem whereby it is difficult to accurately quantify risks to adequate insurance premiums (Young et al. 2016). Organizations that choose a cyberinsurance insurance product may discover that it does not cover a new cyber security risk. Hence, organizations with this understanding can work with their insurers to design policies that accommodate the potential for such changes. It is believed that cyberinsurance can act as an incentive to increase cybersecurity best practices in organizations (Bolot and Lelarge 2009; Gordon et al. 2003). Insurance companies require that client organizations are subject to initial and periodic assessments to determine that minimal or certain security controls (e.g., encryption, anti-virus, backups) are in place in order to be eligible for initial or continuous coverage (Majuca et al. 2006; Young et al. 2016). Insurance companies are known to deny cybersecurity claims when organizations renege from following security best practices. For example, Cottage Health System was denied insurance claim when its insurance company found out that the healthcare organization did not adequately perform encryption to protect its patients records, which was deemed a minimum required practice (Larose and Burke 2015). In addition, there is a practice in the insurance industry that offers reduced premiums/rates in exchange for increased levels of self-protection. Home and automobile insurance providers may offer discounts for anti-theft and fire prevention mechanisms (e.g. smoke detectors, fire extinguishers, burglar alarms). Cyberinsurance carriers can promote security best practices by offering reduced premiums when organizations adhere to or implement security best practices (Gordon et al. 2011). Put together, cyberinsurance coverage requirements and discounts offered for self-protective measures serve to encourage continuous security best practices in organizations. Considering this, organizations should take advantage of cyberinsurance to motivate sustainable security best practices.

Cyberinsurance is usually offered as a standalone product since traditional commercial insurance excludes cyber related risk from policies. Hence, organizations that depend on traditional lines to cover their security risks may be in for some surprises. For example, Sony’s insurance carrier, Zurich American Insurance Co had filed suit against Sony alleging that its policy did not cover damages due to the security breaches, but only covered tangible loses from property damages (McNicholas 2013). Considering that cyberinsurance covers information security risks such as denial-of-service attacks, extortions, malware, legal, breach notification costs, and forensic activities, organizations should actively adopt standalone cyberinsurance policies to protect against such exposure.

3.7.3 Limitations

There are several limitations to the study that warrant consideration. Even though the survey participants (Presidents and CEOs of their respective firms) were ideal as participants for this research, some variance in their positions may have provided different insights. Another possible limitation is that respondents to this study self-reported their commitment towards cyberinsurance. Even though the respondents are executive level leaders in their organizations and were informed that there no right or wrong answers, it is possible that some concealed their true commitments because they wanted to be perceived as socially desirable (Trevino 1992). In this paper, risk perception is conceptualized as breach risk severity. Risk decision-making literature has argued that risk severity and risk susceptibility are important factors in determining the individuals risk perception. Since we did not consider these factors, future research could investigate how risk susceptibility influences the top manager's commitment to cyberinsurance. Finally, this study focused on some individual, organizational, and environmental factors, but future research might investigate the impact of other organizational factors (e.g. sanctions, litigation, and tax benefits) and individual factors (e.g., executive litigation, good image, reputation).

Building on the findings, a critical future research direction is to incorporate job security as a personal relevance factor in security motivation research to increase our understanding of its impact on employee secure behaviors. Another avenue for further research is to investigate the relationship between the adoption of cyberinsurance and implementation of security best practices in organizations. Finally, future research could examine how organization choose which risk management approach to engage in the organization.

APPENDIX A

SUPPLEMENTAL ITEMS FOR ESSAY 1

A.1 Severity Coding

This paper follows for the most part, the Q-sort procedure suggested by Moore and Benbasat (1991). Seven students from a combined master's and undergraduate level information security class judged the topics and severity placement. The judges were informed of the topic categories extracted through text-mining. Then, there were asked to sort the extracted topics according to their severity on a scale of 1 to 5: 1 being not at all severe and 5 being extremely severe. The scaling of severity are based on Ransbotham and Mitra (2009). To assess the reliability of the sorting conducted by the judges, Cohen's kappa was referred to. A kappa score of 0.65 or larger is considered acceptable. The inter-rater reliability (IRR) using Cohen's kappa (Cohen 1960) was .80, indicating adequate agreement. Table A.1 shows the topics extracted. Table A.2 shows IRR statistics, computed using *AgreeStat*, a VBA macro program available from http://agreestat.com/.

Table A.4 reports the correlations between the social capital variables. Though the network measures are highly correlated, we note that social capital measures tend to be highly related (Nahapiet and Ghoshal 1998). In addition, there are no collinearity issues with the independent variables considered for our models (highest VIF is 3.24).

Table A.1: Topics

Extracted Topic	Terms	Docs	Description	Severity
member, post, hh, forum, topic	164	402	Rules and norms	1
hidden, login, content, register, hidden content	12	230	Rules and norms	1
download, file, attach, kb, rar	58	336	Download links	5
found, virus, antivirus, security, scan	118	190	Test antivirus	4
key, value, function, char, int	232	288	Key generators	4
crack, version, update, delphi, install	125	399	Crack software	3
pm, jabber, price, buy, btc	127	298	Bitcoin purchase	1
work, great, x64, test, fine	97	505	Test code	4
server, ip, problem, proxy, check	217	410	Connectivity	1
clean, antivirus, internet, want, result	107	120	Anti-virus test	4
source, code, rat, sell, source code	153	454	RAT source code	5
help, file, dll, look, exe	137	538	Connectivity	2
code, api, help, function, vb6	190	448	Connectivity	2
file, exe, windows, x64, section	201	505	Test code	4
link, post, edit, download, remove	129	360	Download links	5
learn, program, language, section, code	200	458	Programming	1

Table A.2: Inter-Rater Reliability Coefficients and Associated Standard Errors

		Conditional/Rater Sample		Conditional/Subject Sample		Unconditional	
Method	Estimate	Std Error	95% C.I.	Std Error	95% C.I.	Std Error	95% C.I.
AC_1	0.809763	0.129359	(0.517 : 1)	0.01478	(0.776 : 0.843)	0.129766	(0.516 : 1)
AC_{1C}	0.811111	0.126652	(0.525 : 1)	0.01438	(0.779 : 0.844)	N/A	N/A
Kappa	0.800799	0.127753	(0.512 : 1)	0.01730	(0.762 : 0.84)	0.128377	(0.51 : 1)
KappaC	0.7993	0.134286	(0.496 : 1)	0.01777	(0.759 : 0.84)	N/A	N/A
BP	0.808036	0.129053	(0.516 : 1)	0.01524	(0.774 : 0.843)	0.129496	(0.515 : 1)
Conger	0.801294	0.131818	(0.503 : 1)	0.01712	(0.763 : 0.84)	N/A	N/A

Table A.3: Social Capital Factors on PostCount and PostSeverity (Whites and Newey)

	PostCount		**PostSeverity**	
	White's estimation (heteroscedasticity consistent)	**Newey-West estimated (heteroscedasticity and autocorrelation consistent)**	**White's estimation (heteroscedasticity consistent)**	**Newey-West estimated (heteroscedasticity and autocorrelation consistent)**
Betweenness	0.0024692*** (0.00052)	0.0024692*** (0.00052)	-0.000005** (0.000002)	-0.000005** (0.000002)
Degree	0.2028047*** (0.00270)	0.2028047*** (0.00270)	-0.0002107 *** (0.00003)	-0.0002107 *** (0.00003)
Norm	11.50776*** (0.15234)	11.50776*** (0.15234)	0.0044392 *** (0.001)	0.0044392 *** (0.001)
Status	13.46421*** (0.76692)	13.46421*** (0.76692)	0.0159207 (0.01777)	0.0159207 (0.01777)
Tenure	0.0359135*** (0.00191)	0.0359135*** (0.00191)	-0.0004434*** (0.00007)	-0.0004434*** (0.00007)
BoundarySpan	7.544179*** (2.45265)	7.544179*** (2.4526)	-0.6473392*** (0.09425)	-0.6473392*** (0.09425)

Note. Standard errors are in parentheses. p-value < 0:01; *** p-value < 0:001

Table A.3: Correlations of Endogenous Regressors

	DegreeCentrality	**ThreadCount**	**ThreadStarted**
DegreeCentrality	1		
ThreadCount	0.3081	1	
ThreadStarted	0.4496	0.2671	1

Table A.4: Spearman's Correlation Coefficients

	Betweenness	Degree	Norm	Status	Tenure	BoundarySpan
Betweenness	1.0000					
Degree	0.8766*	1.0000				
Norm	0.6513*	0.6315*	1.0000			
Status	0.6216*	0.6234*	0.5579*	1.0000		
Tenure	0.4394*	0.4766*	0.4188*	0.5483*	1.0000	
BoundarySpan	-0.1582*	-0.3746*	-0.1507*	-0.2414*	-0.1031*	1.0000

Note: * P <0.001

APPENDIX B

SUPPLEMENTAL ITEMS FOR ESSAY 2

Please indicate your tendency to accept these risks in using the Internet and computers:

Construct	Measure	Mean	SD	Source
Computer risk propensity	Your computer may be altered accidentally	3.59	1.63	(Chen et al. 2011)
	Your computer may be exploited for malicious purpose (e.g. hackers control and use your computer for spreading worm)	3.39	1.75	
	Your personal identity may be stolen (e.g. Social Security Number SSN)	3.18	1.95	
	Your financial account information (e.g. account/PIN) may be stolen	3.14	1.93	
	Your service account information (email account/password) may be stolen	3.25	1.92	
	It is likely that I will lose sensitive information due to a malware attack	4.34	1.54	
Malware risk severity	I believe that information stored on my computer is vulnerable to malware attacks	4.35	1.46	(Herath and Rao 2009b)
	I believe my personal information (e.g. SSN, password, financial information) stored on my computer is threatened by malware attacks	4.28	1.57	
	My decision to click-through to website links from [Amazon.com/ the source] is risky	4.09	1.57	
Malware risk perception	There is a high potential for loss involved by clicking through to website links from [Amazon.com/ the source]	4.07	1.46	(Chen et al. 2011)
	Clicking through to website links will lead to considerable risks of malware	4.40	1.45	
	I am familiar with searching for product information on the [Amazon.com / source] website	5.38	1.46	
Familiarity	I am familiar with clicking through to product information from the [Amazon.com / source] website	5.22	1.46	(Gefen 2000)
	(table continues)			
	I am familiar with the [Amazon.com/the source] website’s search results	5.44	1.40	

Construct	Measure	Mean	SD	Source
	I am familiar with clicking through to websites suggested on the [Amazon.com/the source website] search results	5.43	1.35	
	I am familiar with [Amazon.com/the source website]'s search results	5.04	1.54	
	Even if not monitored, I'd trust [Amazon.com/the source website] to do the job right	4.80	1.48	
Trust	I trust [Amazon.com/the source website]	5.05	1.38	(Gefen 2000)
	[Amazon.com / the source website] is trustworthy	5.09	1.36	
	[Amazon.com / the source website] is reliable	5.19	1.29	
	I intend to click-through to [websites/target website] suggested to me by [Amazon.com / source site]	3.81	1.62	
Intention to click-through	I am likely to click-through to [websites/target website] from [Amazon.com /source site] search results	3.95	1.58	(Ajzen 1991; Davis 1989)
	I plan to click-through to website results from [Amazon.com / the source]	3.84	1.60	
	I would use my credit card to purchase from the suggested [websites/target website]	3.82	1.74	
	I am very likely to buy from the suggested [websites/target website]	3.73	1.72	
	I feel confident handling malware infected files	3.48	1.81	
Self-efficacy of information security	I feel confident getting rid of malware	3.71	1.79	(Rhee et al. 2009)
	I feel comfortable in my abilities to identify malware files/programs that may be masked	4.16	1.66	
	I feel confident in my abilities to identify websites that are authentic based on the content of the website	4.48	1.61	

Scenario Design

Two different scenarios are used to access the behavioral intentions of individuals towards click-through over two seemly different sites: a highly trusted website such as Amazon.com and the subjects' self-selected search engine site. In so doing, we access whether their behavioral intentions towards click-through will differ based on the trust of the sites. Thus, we measure the variations in the dependent variable which is a critical requirement for statistical testing of hypotheses Bhattacherjee (2002). The questionnaires were mostly identical baring the difference in the source sites. The first scenario entails the explicit use of Amazon.com as the source site. The second scenario is similar to the first, the difference entails a search engine site as the source site. ComputerWorld (2010) describes a situation similar to the search engine scenario, in which users perform a search on Google, and the search result includes links to malicious sites. Also, Im et al. (2016) examine the behavior of online consumers who seek "great deals" in the form of low prices (e.g. bargain hunters).

Scenario A: Amazon.com

Assume that you have logged into Amazon.com to find and purchase a wedding gift for a friend. You type in the name of the wedding gift item, and the search results are displayed. In the results you notice that the item you want is sold only by sellers linked to Amazon. This means that there are links on the product information indicating that you click through to the sellers' website in order to purchase the product.

Scenario B: Self-selected search engine site

Assume that you performed a search on a search engine (e.g. Bing, Google, Yahoo!, Ask etc.) to find and purchase a wedding gift for a friend. You type in the name of the wedding gift item in a search engine, and the search results are displayed. In the results, you notice a link with a fairly good price. The link indicates that you click through to the seller's website in order to purchase the product.

APPENDIX C

SUPPLEMENTAL ITEMS FOR ESSAY 3

Survey Instruments and Questions

Table C.1: Items for Constructs and CFA Factor Loadings

		Loading	STD	p-value	Mean	STD
Ambiguity 1–7: Strongly Disagree to Strongly Agree						
AMB1	It is difficult to understand what risks are being insured through cyberinsurance	0.881	0.152	0.000	4.62	1.806
AMB2	There is often a lack of common language in the meaning of cyber incidents covered in cyberinsurance	0.959	0.147	0.000	4.96	1.645
AMB3	There is difficulty in fully understanding the risk and appropriate cyberinsurance coverage	0.93	0.133	0.000	4.91	1.675
AMB4	There is a lack of clarity about the limits of coverage on cyberinsurance policies	0.932	0.131	0.000	4.94	1.690
Commitment 1–7: Strongly Disagree to Strongly Agree						
COMM 1	I am committed to supporting efforts in adopting cyberinsurance for managing security risks	0.951	0.011	0.000	5.56	1.508
COMM 2	I encourage the use of cyberinsurance for managing security risks	0.934	0.015	0.000	5.56	1.436
COMM 3	I am committed to a vision of adopting cyberinsurance for managing security risks	0.954	0.01	0.000	5.48	1.544
COMM 4	The use of cyberinsurance for managing security risks is important to our organization	0.922	0.02	0.000	5.55	1.473
Financial Risk 1–7: Strongly Disagree to Strongly Agree						
FIN1	Lead to a financial loss due to notifying affected individuals, public relations, fines etc.	0.885	0.025	0.000	5.25	1.693
FIN2	… Subject our organization to financial loss	0.842	0.041	0.000	5.64	1.421

(table continues)

		Loading	STD	p-value	Mean	STD
FIN3	… Lead to a financial loss due to reimbursing customers for fraudulent charges	0.884	0.026	0.000	5.24	1.780
FIN4	… Expose our organization to suffer financial loss due to reporting requirements or legal fines	0.869	0.025	0.000	5.09	1.803
FIN45*	… Lead to a financial loss due to lost revenue	0.821	0.051	0.000	5.55	1.522
Job Security 1–7: Strongly Disagree to Strongly Agree						
JSEC1	Cyberinsurance protection will protect my job	0.937	0.016	0.000	5.26	1.610
JSEC2	Cyberinsurance protection will help control the undesirable events that might affect my job	0.926	0.015	0.000	5.60	1.524
JSEC3	Cyberinsurance protection will offer me continued long term job security	0.952	0.012	0.000	5.26	1.636
Regulatory Oversight Risk 1–7: Strongly Disagree to Strongly Agree						
REG1	… Defines specific operational activities that must be followed by our organization	0.884	0.03	0.000	4.69	2.001
REG2	… Oversees and supervises our organization's operations and actions	0.907	0.02	0.000	4.24	2.172
REG3	… Specifies objectives and outcome criteria that governs our operations (e.g. data breach notification)	0.945	0.011	0.000	4.44	2.045
REG4	… Takes action to hold our firm accountable for the performance and safety of our products and	0.878	0.028	0.000	4.87	2.001
REG5	… Works closely with our firm to remedy and conform to regulated actions (e.g. data breach notification)	0.908	0.018	0.000	4.28	2.143

(table continues)

		Loading	STD	p-value	Mean	STD
Security Breach Perception 1–7: Strongly Disagree to Strongly Agree						
SEV2	If our organization's business operations were to be disrupted from a security breach, it would be severe	0.897	0.021	0.000	5.35	1.524
SEV3	If our organization were to lose customers from a security breach, it would be serious	0.858	0.054	0.000	5.86	1.414
SEV4	If our organization were to cover the costs of a security breach incident, it would be significant	0.943	0.01	0.000	5.67	1.436
SEV5*	If our organization's security is breached, it would be expensive to recover	0.895	0.02	0.000	5.52	1.469
Transaction Cost 1–7: Strongly Disagree to Strongly Agree						
TXNC1	The cost of negotiating a cyberinsurance contract would be too much	0.894	0.215	0.000	4.13	1.812
TXNC2	The cost of monitoring and verifying the cyberinsurance contract details would be too much	0.835	0.226	0.000	4.21	1.913
TXNC3	The cost of transferring knowledge about our organization's security to the cyberinsurance company would be too much	0.76	0.255	0.003	4.13	1.812
TXNC4	In general, it would be a hassle contracting with a cyberinsurance company	0.974	0.254	0.000	4.14	1.929

Table C.2: Questionnaire Items for Demographics and Control

		Mean	STD
InfoSec Management	How many years experience do you have in information security management?	7.91	6.23
Technology management	How many years experience do you have in technology management?	8.78	6.16
Tenure	How many years have you been in your current position?	10.47	7.69

Instrument Design and Development

This paper follows the Q-sort procedure suggested by Moore and Benbasat (1991). Four Ph.D. students sorted items for the regulatory oversight risk construct. To assess the reliability of the sorting conducted by the judges, we referred to Cohen’s kappa was referred. A kappa score of 0.65 or larger is considered acceptable. The inter-rater reliability (IRR) using Cohen's kappa (Cohen 1960) was 0.93, indicating adequate agreement. Table C.3 shows IRR statistics, computed using *AgreeStat*, a VBA macro program available from http://agreestat.com/

Table C.3: Questionnaire Items for Demographics and Controls

		Conditional/Rater Sample		**Conditional/Subject Sample**		**Unconditional**	
Method	Estimate	Std Error	95%C.I.	Std Error	95% C.I.	Std Error	95% C.I.
AC1	0.933	0.0706	(0.766 : 1)	0.0679	(0.773 : 1)	0.07775	(0.75 : 1)
AC1C	0.933	0.0669	(0.775 : 1)	0.0677	(0.773 : 1)	N/A	N/A

Reliability and Validation

Prior to examining the structural model, we evaluated general information (means, standard deviations, correlations, variance inflation factor, and its tolerance index) about the model (see Table C.4). The variance inflation factor (VIF) was used to ensure there were no issues with multicollinearity. The values were below the most conservation thresholds 3 (Diamantopoulos 2006). The Durbin-Watson statistic is 1.94, which is between 1.5 and 2.5 and therefore the data is not autocorrelated. Given that this study is an exploratory, we performed an exploratory factor analysis (see Table C.5). For the exploratory factor analysis, we used principal components analysis with varimax rotations. We removed any item with low factor loading and high cross loading (Job Security). The item is noted in Appendix A with an asterisk and was deleted prior to performing the subsequent measurement analysis.

We performed reliability analysis and its results are provided in Table C.6. Cronbach's α for each construct are above the recommended value of .70 (Hair et al. 2006) and ranges from 0.908 (FIN) to 0.9564 (COMM). Composite reliability ranges from 0.9246 (TXNC) to 0.9684 (COMM). Average variance extracted (AVE) for each construct exceeds 0.50 (Chin 1998; Fornell and Larcker 1981), and ranges from 0.7305 (FIN) to 0.8845 (COMM), which fulfils the requirement for convergent validity.

To evaluate the discriminant validity of the constructs, we followed two approaches. First, we used the approach recommended by Fornell and Larcker (1981). The results of the analysis is provided in Table C.7 and indicates that each construct's AVE is greater than the squared correlation between each pair of constructs in the model. In addition, we assess discriminant validity using the heterotrait–monotrait ratio (HTMT) approach suggested by Henseler et al. (2014). There are two ways of assessing discriminant validity using the HTMT method. First, compare whether the HTMT value is below a recommended threshold. Second, using a confidence interval, we test a HTMT null hypothesis of equal to or more than 1. The results of the first test shows that the highest absolute value for our measures is 0.79 (see Table C.8) and satisfies a conservative threshold of 0.85 (Henseler et al. 2014). In the second test, all upper confidence intervals are below the value of 1, suggesting that the HTMT values are significantly different from 1 (see Table C.9). Therefore, we conclude that discriminant validity of the measurement model is achieved.

To address potential common methods bias in the survey design, we use methodologically separate measures to crease a psychological separation by using different response formats such as sematic differential, Likert scales, and open-ended questions. The benefit of using the different formats is that it tends to reduce response biases in by “eliminating the saliency of contextually provided cues” (Podsakoff et al. 2003, p. 888). In addition, Podaskoff et al. (2003) note that the cover should inform participants that the survey is anonymous and that there are no right or wrong answers. Hence, respondents were informed in the cover of the anonymous nature of the survey and that there were no right or wrong answers.

We assessed the extent of common methods variance (CMV) in the data using two methods. First, we performed Harmon’s one factor test (Podsakoff et al. 2011) by including all reflective-items in a principal components factor analysis. The results revealed six factors with no single factor accounting for a majority of variance (i.e., the largest factor variance was 38.5%).

Furthermore, researchers suggest that a factor based PLS-SEM full collinearity test can be used to assess common method bias (Kock 2015; Kock and Lynn 2012). Factor based PLS-SEM algorithm differs from classic PLS-SEM algorithm. Because classic PLS-SEM algorithm maximizes variance, it tends to minimize model collinearity. Variance maximization happens because classic PLS-SEM algorithm does not model measurement errors. Since factor-based PLS-SEM incorporates measurement errors, it is less of a problem. Performing a factor based full collinearity test shows that the highest VIF of all latent constructs is 3.78. This is below the threshold of 5 (Kline 1998; Kock 2015) and suggests that CMV is not a major problem in this study.

Finally, we used Stone (1974) and Geisser’s (1974) cross-validated redundancy measure Q^2, to assess the model’s predictive relevance. The Q-squared coefficient is a nonparametric measure used for assessing the predictive validity related to each variable in a path model and the endogenous dependent variable in the path model (Kock and Gaskins 2014). *Q*-squared coefficients that are greater than zero suggest an acceptable predictive validity in the relationship between the variables and the dependent variable. Our model presents acceptable predictive validity since the *Q*-squared coefficients in the model are greater is 0.565.

Table C.4. Descriptive Statistics (n = 151)

	COMM	AMB	FIN	REG	TXNC	SEV	JSEC
COMM	1						
AMB	0.093	1					
FIN	0.598**	0.211**	1				
REG	0.485**	0.137	0.442**	1			
TXNC	-0.066	0.555**	0.135	0.252**	1		
SEV	0.629**	0.243**	0.645**	0.337**	0.155	1	
JSEC	0.752**	0.068	0.486**	0.529**	0.023	0.580**	1
Mean	5.5868	4.8874	5.3523	4.5706	4.1507	5.6269	5.3753
SD	1.36287	1.55307	1.40565	1.83540	1.72749	1.31427	1.49235
VIF		1.519	1.915	1.623	1.560	2.135	1.941
Tolerance		0.658	0.522	0.616	0.641	0.468	0.515

**Correlation Significant at .01 Level. Table Legend: COMM = Commitment towards using Cyberinsurance as a Risk Management Strategy; AMBG = Ambiguity of Cyberinsurance; FIN= Financial Risk; REG = Regulation Oversight Risk; TXNCN = Transaction Cost; SEV = Breach Risk Severity; JSEC = Job Security

Table C.5: Exploratory Factor Analysis

	COMM	AMBG	FIN	REG	TXNC	SEV	JSEC
COMM1	0.778						
COMM2	0.827						
COMM3	0.808						
COMM4	0.848						
COMM5	0.776						
AMBG1		0.869					
AMBG2		0.882					
AMBG3		0.876					

(table continues)

	COMM	AMBG	FIN	REG	TXNC	SEV	JSEC
AMBG4		0.906					
AMBG5		0.841					
FIN1			0.724				
FIN2			0.771				
FIN3			0.774				
FIN4			0.727				
FIN5			0.784				
REG1				0.879			
REG2				0.866			
REG3				0.871			
REG4				0.844			
REG5				0.828			
REG6				0.738			
TXNC3					0.827		
TXNC4					0.894		
TXNC5					0.853		
TXNC6					0.821		
SEV2						0.705	
SEV3						0.825	
SEV4						0.728	
JSEC1							0.719
JSEC2							0.700
JSEC3							0.728

Note: Loadings less than 0.5 are omitted from the table for clarity

Table C.6. Convergent Validity Summary and Construct Reliabilities

	Average Variance Extracted		Cronbach’s Alpha
AMB	0.8163	0.9568	0.9483
COMM	0.8845	0.9684	0.9564
FIN	0.7305	0.9313	0.908
JSEC	0.8803	0.9566	0.932

(table continues)

	Average Variance Extracted		Cronbach's Alpha
REG	0.8181	0.9574	0.9444
SEV	0.7836	0.9353	0.9084
TXNC	0.7556	0.9246	0.944

Table Legend: COMM= Commitment towards using Cyberinsurance as a Risk Management Strategy; AMBG = Ambiguity of Cyberinsurance; FIN= Financial Risk; REG = Regulation Oversight Risk; TXNC = Transaction Cost; SEV = Breach Risk Severity; JSEC = Job Security

Table C.7: Correlations Among Latent Constructs

	AMB	COMM	FIN	JSEC	REG	SEV	TXNC
AMB	0.9035	0	0	0	0	0	0
COMM	0.1234	0.9405	0	0	0	0	0
FIN	0.2151	0.5994	0.8547	0	0	0	0
JSEC	0.1046	0.7521	0.489	0.9382	0	0	0
REG	0.1438	0.4933	0.4219	0.5137	0.9045	0	0
SEV	0.253	0.6733	0.6502	0.6069	0.3341	0.8852	0
TXNC	0.5163	-0.1639	0.0509	-0.0683	0.1646	0.0636	0.8693

Note**:** The diagonals are the square root of the average variance extracted (AVE) for each factor. Table Legend: COMM= Commitment towards using Cyberinsurance as a Risk Management Strategy; AMBG = Ambiguity of Cyberinsurance; FIN= Financial Risk; REG = Regulation Oversight Risk; TXNCN = Transaction Cost; SEV = Breach Risk Severity;JSEC = Job Security

Table C.8: Heterotrait-Monotrait Ratio of the Correlations (HTMT)

	AMB	COMM	FIN	JSEC	REG	SEV
COMM	0.119					
FIN	0.221	0.638				
JSEC	0.102	0.795	0.521			
REG	0.156	0.516	0.445	0.549		
SEV	0.274	0.675	0.72	0.639	0.361	
TXNC	0.586	0.091	0.15	0.075	0.274	0.17

Table C.9: Confidence Intervals of HTMT

	Original Sample	Sample Mean	2.50%	97.50%
COMM → AMB	0.119	0.145	0.05	0.296
FIN → AMB	0.221	0.238	0.086	0.423
FIN → COMM	0.638	0.639	0.463	0.793
JSEC → AMB	0.102	0.127	0.04	0.284

(table continues)

	Original Sample	Sample Mean	2.50%	97.50%
JSEC → COMM	0.795	0.794	0.69	0.885
JSEC → FIN	0.521	0.522	0.344	0.678
REG → AMB	0.156	0.169	0.057	0.331
REG → COMM	0.516	0.518	0.393	0.629
REG → FIN	0.445	0.444	0.259	0.62
REG → JSEC	0.549	0.55	0.416	0.674
SEV → AMB	0.274	0.281	0.105	0.478
SEV → COMM	0.675	0.675	0.561	0.779
SEV → FIN	0.72	0.726	0.588	0.858
SEV → JSEC	0.639	0.639	0.498	0.765
SEV → REG	0.361	0.363	0.179	0.529
TXNC → AMB	0.586	0.585	0.447	0.698
TXNC → COMM	0.091	0.119	0.061	0.217
TXNC → FIN	0.15	0.178	0.073	0.331
TXNC → JSEC	0.075	0.114	0.055	0.225
TXNC → REG	0.274	0.277	0.121	0.447
TXNC → SEV	0.17	0.182	0.068	0.351

Table Legend: COMM= Commitment towards using Cyberinsurance as a Risk Management Strategy; AMBG = Ambiguity of Cyberinsurance; FIN= Financial Risk; REG = Regulation Oversight Risk; TXNCN = Transaction Cost; SEV = Breach Risk Severity; JSEC = Job Security

REFERENCES

Abbasi, A., Li, W., Benjamin, V., Hu, S., and Chen, H. 2014. "Descriptive Analytics: Examining Expert Hackers in Web Forums," in *IEEE Joint Intelligence and Security Informatics Conference*, The Hague: IEEE.

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker Jr, J. F. 2010. "Detecting fake websites: the contribution of statistical learning theory," *MIS Quarterly*, pp. 435–461.

Absolute. 2015. "IT Confidential - The State of security confidence.,"

Acquisti, A., Friedman, A., and Telang, R. 2006. "Is there a cost to privacy breaches? An event study," *ICIS 2006 Proceedings*, p. 94.

Adams, M., Lin, C., and Zou, H. 2011. "Chief executive officer incentives, monitoring, and corporate risk management: Evidence from insurance use," *Journal of Risk and Insurance* (78:3), pp. 551–582 (doi: 10.1111/j.1539-6975.2011.01409.x).

Adler, P. S., and Kwon, S. 2002. "Social Capital: Prospects for a New Concept," *Academy of Management Review* (27:1), pp. 17–40.

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

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Ajzen, I., and Brown, T. 1996. "Information bias in contingent valuation: effects of personal relevance, quality of information, and motivational orientation," *Journal of Environmental Economics and Management* (30), pp. 43–57.

Ajzen, I., and Fishbein, M. 1977. "Attitude-behavior relations: A theoretical analysis and review of empirical research," *Psychological Bulletin* (84:5), p. 888.

Akhawe, D., and Felt, A. 2013. "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness.," *Usenix Security*.

Albarracín, D., and Kumkale, G. T. 2003. "Affect as information in persuasion: a model of affect identification and discounting.," *Journal of personality and social psychology* (84:3), pp. 453–469 (doi: 10.1037/0022-3514.84.3.453).

Aldrich, H., and Herker, D. 1977. "Boundary Spanning roles and Organization Structure.," *Academy of Management Review* (2:2), pp. 217–230.

Allen, T. J. 1977. *Managing the flow of technology: Technology transfer and the dissemination of technological information within the R&D organization*, Cambridge, MA: MIT Press.

Ang, S., and Straub, D. W. 1998. "Production and Transaction Economies and IS Outsourcing: A Study of the U. S. Banking Industry," *MIS Quarterly* (22:4), p. 535 (doi: 10.2307/249554).

Artz, D., and Gil, Y. 2007. "A survey of trust in computer science and the semantic web," *Web Semantics: Science, Services and Agents on the World Wide Web* (5:2), pp. 58–71.

Ashford, S. J., Lee, C., and Bobko, P. 1989. "Content, Cause, and Consequences of Job Insecurity: a Theory-Based Measure and Substantive Test.," *Academy of Management Journal* (32:4), pp. 803–829 (doi: 10.2307/256569).

Bandura, A. 1998. "Health promotion from the perspective of social cognitive theory," *Psychology and health* (13:4), pp. 623–649.

Bandyopadhyay, T., Mookerjee, V. S., and Rao, R. C. 2009. "Why IT managers don't go for cyber-insurance products," *Communications of the ACM* (52:11), p. 68 (doi: 10.1145/1592761.1592780).

Belliveau, M. A., O'Reilly, C. A., and Wade, J. B. 1996. "Social capital at the top: Effects of social similarity and status on CEO compensation," *Academy of Management Journal* (39:6), pp. 1568–1593.

Benaroch, M., and Fink, L. 2016. "Contract design choices and the balance of ex ante and ex post transaction costs in software development outsourcing," *MIS Quarterly* (40:1), pp. 57–82.

Benjamin, V., and Hsinchun Chen. 2012. "Securing cyberspace: Identifying key actors in hacker communities," in *2012 IEEE International Conference on Intelligence and Security Informatics*, IEEE, June, pp. 24–29.

Benjamin, V., Li, W., Holt, T., and Chen, H. 2015. "Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops," *Intelligence and Security*.

Benjamin, V., Zhang, B., Nunamaker, J. F., and Chen, H. 2016. "Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities," *Journal of Management Information Systems* (33:2), pp. 482–510.

Bertrand, M., and Schoar, A. 2003. "Managing With Style: The Effect of Managers on Firm Policies," *Social Science Research* (August).

Bhattacherjee, A. 2002. "Individual trust in online firms: Scale development and initial test," *Journal of Management Information Systems* (19:1), pp. 211–241.

Bitektine, A. 2011. "Toward a Theory of Social Judgments of Organizations: the Case of Legitimacy, Reputation, and Status," *Academy of Management Review* (36:1), pp. 151–179.

Böhme, R., and Kataria, G. 2006. "On the limits of cyber-insurance," in *Trust and Privacy in Digital Business*, Springer, pp. 31–40.

Böhme, R., and Schwartz, G. 2010. "Modeling Cyber-Insurance: Towards a Unifying Framework," in *WEIS*.

Bolot, J., and Lelarge, M. 2009. "Cyber Insurance as an Incentivefor Internet Security," in *Managing information risk and the economics of security*, Springer, pp. 269–290.

Boo, E., and Sharma, D. 2008. "Effect of regulatory oversight on the association between internal governance characteristics and audit fees," *Accounting and Finance* (48:1), pp. 51–71 (doi: 10.1111/j.1467-629X.2007.00229.x).

Borgatti, S., Everett, M., and Freeman, L. 2002. "UCINET for Windows: Software for social network analysis," *Harvard, MA: Analytic Technologies* (available at https://sites.google.com/site/ucinetsoftware/home).

Borges Hink, R. C., and Goseva-Popstojanova, K. 2016. "Characterization of Cyberattacks Aimed at Integrated Industrial Control and Enterprise Systems: A Case Study," *Proceedings of IEEE International Symposium on High Assurance Systems Engineering*, pp. 149–156.

Bose, I., and Leung, A. C. M. 2014. "Do phishing alerts impact global corporations? A firm value analysis," *Decision Support Systems* (64), Elsevier B.V., pp. 67–78 (doi: 10.1016/j.dss.2014.04.006).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly (May-2015 Forthcoming).*

Bourdieu, P. 1986. "The forms of capital," in *Handbook of Theory and Research for the Sociology of Education*J. . Richardson (ed.), Westport, CT: Greenwood Press.

Briggs, R., and Hollis, N. 1997. "Advertising on the web: Is there response before click-through?," *Journal of Advertising research*.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (34:3), pp. 523–548.

Burt, R. S. 1992. *Structural holes: The social structure of competition*, Cambridge, MA: Harvard University Press.

Burt, R. S. 1997. "The Contingent Value of Social Capital," *Administrative Science Quarterly* (42:2), p. 339.

Burt, R. S. 2000. "The Network Structure of Social Capital," *Research in Organizational Behaviour* (22), Elsevier Masson SAS, pp. 345–423.

Cacioppo, J. T., Petty, R. E., Feinstein, J. A., and Jarvis, W. B. G. 1996. "Dispositional differences in cognitive motivation: The life and times of individuals varying in need for cognition," *Psychological Bulletin* (119:2), p. 197.

Calka, M. 2006. "Beyond Newbie: Immersion In Virtual Game Worlds.,"

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security* (11:3), pp. 431–448.

Campo, S., and Cameron, K. a. 2006. "Differential Effects of Exposure to Social Norms Campaigns : A Cause for Concern Differential Effects of Exposure to Social Norms Campaigns : A Cause for Concern," *Health Communication* (19:3), pp. 209–219.

Carson, S. J., Madhok, A., and Tao, W. 2006. "Uncertainty, opportunism, and governance: The effects of volatility and ambiguity on formal and relational contracting," *Academy of Management Journal* (49:5), pp. 1058–1077 (doi: 10.5465/AMJ.2006.22798187).

Cavusoglu, H., Mishra, B., and 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), pp. 70–104.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The value of intrusion detection systems in information technology security architecture," *Information Systems Research* (16:1), pp. 28–46.

Chang, C.-M., Hsu, M.-H., and Lee, Y.-J. 2015. "Factors Influencing Knowledge-Sharing Behavior in Virtual Communities: A Longitudinal Investigation," *Information Systems Management* (32:4), pp. 331–340.

Chantler, A. N. 1995. "Risk: The profile of the computer hacker," Curtin University of Technology.

Chen, R., Wang, J., Herath, T., and Rao, R. 2011. "An investigation of email processing from a risky decision making perspective," *Decision Support Systems* (52:1), pp. 73–81.

Chin, W. W. 1998. "Commentary: Issues and opinion on structural equation modeling," JSTOR.

Cho, J., and Lee, J. 2006. "An integrated model of risk and risk-reducing strategies," *Journal of Business Research* (59:1), pp. 112–120.

Choudhury, V., and Sampler, J. L. 1997. "Information Specificity and Environmental Scanning: An Economic Perspective," *MIS Quarterly* (21:1), p. 25 (doi: 10.2307/249741).

Cohen, D., and Prusak, L. 2001. *In good company: How social capital makes organizations work* (Vol. 15), Harvard Business School Press Boston, MA.

Cohen, J. 1960. "A coefficient of agreement for nominal scales," *Educational and psychological measurement* (20:1), pp. 37–46.

Coleman, J. 1988. "Social capital in the creation of human capital," *American journal of sociology*.

Coleman, J. S. 1990. *Foundations of Social Theory,* Cambridge, MA: The Belknap Press of Harvard University Press.

Collins, M., and Urban, C. 2014. "The dark side of sunshine: Regulatory oversight and status quo bias," *Journal of Economic Behavior and Organization* (107:PB), Elsevier B.V., pp. 470–486 (doi: 10.1016/j.jebo.2014.04.003).

Compeau, D., and Higgins, C. 1995. "Computer self-efficacy: Development of a measure and initial test," *MIS Quartely* (available at http://www.jstor.org/stable/249688).

Computer Security Institute. 2011. "Computer Crime and Security Survey," 2011 (available at http://analytics.informationweek.com/abstract/21/7377/Security/research-2010-2011-csisurvey.html).

ComputerWorld. 2010. "Don't click that link, but if you do...," ComputerWorld (available at http://www.computerworld.com/article/2468755/microsoft-windows/don-t-click-that-link--but-if-you-do---.html).

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

Cross, T. 2006. "Academic Freedon and the Hacker Ethic," *Communications of the ACM* (49:6).

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (32), pp. 90–101.

CSO. 2016. "Data breaches often result in CEO firing," *CSO* (available at http://www.csoonline.com/article/3040982/security/data-breaches-often-result-in-ceo-firing.html; retrieved January 11, 2017).

Cummings, J. N. 2004. "Work groups, structural diversity, and knowledge sharing in a global organization," *Management Science* (50:3), pp. 352–364.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research* (20:1), pp. 79–98.

Daft, R. L., Lengel, R. H., and Trevino, L. K. 1987. "for Information Systems Message Equivocality , Media Selection , and Manager performance : Implications for Information Systems," *MIS Quartely* (11:3), pp. 355–366.

Daft, R., and Macintosh, N. 1981. "A tentative exploration into the amount and equivocality of information processing in organizational work units," *Administrative science quarterly* (available at http://www.jstor.org/stable/2392469).

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319–340 (doi: 10.2307/249008).

Décary-Hétu, D., and Dupont, B. 2012. “The social network of hackers,” *Global Crime* (13:3), pp. 160–175.

Décary-Hétu, D., and Dupont, B. 2013. “Reputation in a dark network of online criminals,” *Global Crime* (14:February), pp. 2–3.

Décary-Hétu, D., Morselli, C., and Leman-Langlois, S. 2012. “Welcome to the Scene: A Study of Social Organization and Recognition among Warez Hackers,” *Journal of Research in Crime and Delinquency* (49:3), pp. 359–382.

Deerwester, S., Dumais, S. T., Furnas, G. W., Landauer, T. K., and Harshman, R. 1990. “Indexing by latent semantic analysis,” *Journal of the American society for information science* (41:6), American Documentation Institute, p. 391.

DELL. 2015. “How to Spot a Fake Website and Not Get Phished ,” Dell.com (available at http://www.dell.com/downloads/ca/support/spot_fake_website_not_get_phished_dell_en.pdf).

DeLooze, L. L. 2004. “Classification of computer attacks using a self organizing map,” *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.*, pp. 365–369.

Department of Homeland Security. 2012. “Cybersecurity Insurance Industry Readout Reports,” (available at https://www.dhs.gov/publication/cybersecurity-insurance-reports).

Desanctis, G. L. 1982. “An Examination of an Expectancy Theory Model of Decision Support System USe.,”

Dey, D., Lahiri, A., and Zhang, G. 2012. “Hacker Behavior, Network Effects, and the Security Software Market,” *Journal of Management Information Systems* (29:2), pp. 77–108.

Dhar, S., and Balakrishnan, B. 2006. “Risks, Benefits, and Challenges in Global IT Outsourcing,” *Journal of Global Information Management* (14:3), pp. 59–89 (doi: 10.4018/jgim.2006070104).

DHS. 2016. “National Cyber Incident Response Plan - December 2016,” (available at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf).

Diamantopoulos, A. 2006. “The error term in formative measurement models: interpretation and modeling implications,” *Journal of Modelling in Management* (1:1), pp. 7–17.

Dibbern, J., Winkler, J., and Heinzl, A. 2008. “Explaining variations in client extra costs between software projects offshored to India,” *MIS Quaterly* (32:2), pp. 333–366 (doi: Article).

Dillard, A. J., Ferrer, R. A., Ubel, P. A., and Fagerlin, A. 2012. “Risk perception measures’ associations with behavior intentions, affect, and cognition following colon cancer screening messages,” *Health psychology* (31:1), p. 106.

Dinev, T. 2006. “Why spoofing is serious internet fraud,” *Communications of the ACM* (49:10), pp. 76–82.

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2012. “Information privacy and correlates : an empirical attempt to bridge and distinguish privacy-related concepts,” *European Journal of Information Systems* (22:3), Nature Publishing Group, pp. 295–316.

Doherty, N. 2000. *Integrated risk management: Techniques and strategies for Managing corporate risk McGraw Hill Professional*.

Dupont, B., Côté, A.-M., Savine, C., and Décary-Hétu, D. 2016. “The ecology of trust among hackers,” *Global Crime* (17:2), Routledge, pp. 129–151.

Experian. 2014. “Data Breach Response,” (available at https://www.experian.com/assets/data-breach/brochures/response-guide.pdf).

Experian. 2015. “Experian Data Breach Industry Forecast,” (available at http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf.).

Experian. 2016. “Facing Greater Risks, Small Businesses Still Lag in Adopting Cyber Insurance,” (available at http://www.experian.com/blogs/data-breach/2016/04/19/facing-greater-risks-small-businesses-still-lag-in-adopting-cyber-insurance/; retrieved October 10, 2016).

Faraj, S., Jarvenpaa, S., and Majchrzak, A. 2011. “Knowledge collaboration in online communities,” *Organization science* (22:5), pp. 1224–1239.

Faraj, S., and Johnson, S. 2011. “Network exchange patterns in online communities,” *Organization Science*.

Feather, N. T. 1988. “Values, valences, and course enrollment: Testing the role of personal values within an expectancy - valence framework.,” *Journal of Educational Psychology* (80:3), pp. 381–391 (doi: 10.1037/0022-0663.80.3.381).

Featherman, M. S., and Pavlou, P. A. 2003. “Predicting e-services adoption: a perceived risk facets perspective,” *International journal of human-computer studies* (59:4), pp. 451–474.

Financial Services Rountable. 2011. “Malware Risks and Mitigation Report,” NIST (available at http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf.).

Finkelstein, S., and Hambrick, D. C. 1990. “Top-Management-Team Tenure and Organizational Outcomes: The Moderating Roie of Managerial Discretion,” *Administrative Science Quarterly* (35:3), pp. 484–503 (doi: 10.2307/2393314).

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., and Combs, B. 1978. “How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits,” *Policy sciences* (9:2), pp. 127–152.

Fleming, L., and Waguespack, D. M. 2007. “Brokerage, Boundary Spanning, and Leadership in Open Innovation Communities,” *Organization Science* (18:2), pp. 165–180.

Forbes. 2014. “Fallout: The reputational impact of IT risk,” (available at https://www-935.ibm.com/services/multimedia/RLL12363USEN_2014_Forbes_Insights.pdf; retrieved November 7, 2016).

Fornell, C., and Larcker, D. F. 1981. “Structural equation models with unobservable variables and measurement error: Algebra and statistics,” *Journal of marketing research*, pp. 382–388.

Fox, F. V., and Staw, B. M. 1979. “The trapped administrator: effects of job insecurity and policy resistance upon commitment to a course of action,” *Administrative Science Quarterly* (24:3), pp. 449–471 (doi: 10.2307/2989922).

Fukuyama, F. 1995. *Trust: The social virtues and the creation of prosperity*, London: Hamish Hamilton.

Furnell, S. 2003. “Cybercrime: Vandalizing the information society,” *Web Engineering, Proceedings* (2722), pp. 8–16.

Furnell, S. M. 2004. “Hacking begins at home: are company networks at risk from home computers?,” *Computer Fraud & Security* (1), pp. 4–7.

Gantz, J., Christiansen, C., and Gillen, A. 2006. “The risks of obtaining and using pirated software,” *IDC*.

Gao, H., Hu, J., Huang, T., and Wang, J. 2011. “Security issues in online social networks,” *IEEE Internet*.

Gardner, M., and Steinberg, L. 2005. “Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study.,” *Developmental psychology*.

Geer, D. 2003. “Risk management is still where the money is,” *Computer* (12), pp. 129–131.

Gefen, D. 2000. “E-commerce: the role of familiarity and trust,” *Omega* (28:6), pp. 725–737.

Gefen, D., Benbasat, I., and Pavlou, P. 2008. “A research agenda for trust in online environments,” *Journal of Management Information Systems* (24:4), pp. 275–286.

Gefen, D., Rao, V. S., and Tractinsky, N. 2003. “The conceptualization of trust, risk and their electronic commerce: the need for clarifications,” in *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, IEEE, p. 10 pp.

Gefen, D., and Straub, D. W. 2004. “Consumer trust in B2C e-commerce and the importance of social presence: experiments in e-products and e-services,” *Omega* (32:6), pp. 407–424.

Geisser, S. 1974. “A predictive approach to the random effect model,” *Biometrika* (61:1), pp. 101–107.

GO-Gulf. 2015. “How People Spend Their Time Online ,” (available at http://www.go-gulf.com/blog/online-time/).

Goel, S., and Shawky, H. A. 2014. “The Impact of federal and state notification laws on security breach announcements,” *Communications of the Association for Information Systems* (34:1), pp. 37–50.

Goodhue, D. L., and Straub, D. W. 1991. “Security concerns of system users,” *Information & Management* (20:1), pp. 13–27.

Goodwin, N. 1996. *Economic meanings of trust and responsibility The University of Michigan*, Ann Arbor, MI: The University of Michigan Press.

Gordon, L. A., Loeb, M. P., and Sohail, T. 2003. “A framework for using insurance for cyber-risk management,” *Communications of the ACM* (46:3), pp. 81–85.

Gordon, L. A., Loeb, M. P., and Zhou, L. 2011. “The impact of information security breaches: Has there been a downward shift in costs?,” *Journal of Computer Security* (19:1), pp. 33–56.

Gray, P. H. 2001. “The Impact of Knowledge Repositories on Power and Control in the Workplace,” *Information Technology & People* (14:4), pp. 368–384.

Grazioli, S., and Jarvenpaa, S. L. 2000. “Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers,” *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* (30:4), pp. 395–410.

Grazioli, S., and Jarvenpaa, S. L. 2003. “Consumer and business deception on the Internet: Content analysis of documentary evidence,” *International Journal of Electronic Commerce* (7:4), pp. 93–118.

Grier, C., Thomas, K., Paxson, V., and Zhang, M. 2010. “@ spam: the underground on 140 characters or less,” in *Proceedings of the 17th ACM conference on Computer and communications security*, ACM, pp. 27–37.

Gu, B., Park, J., and Konana, P. 2012. “The Impact of External Word-of-Mouth Sources on Retailer Sales of High-Involvement Products,” *Information Systems Research* (23:1), pp. 182–196.

Gupta, A., Su, B.-C., and Walter, Z. 2004. “An empirical study of consumer switching from traditional to electronic channels: A purchase-decision process perspective,” *International Journal of Electronic Commerce* (8:3), pp. 131–161.

Haas, M. R., and Park, S. 2010. “To Share or Not to Share? Professional Norms, Reference Groups, and Information Withholding Among Life Scientists,” *Organization Science* (21:4), pp. 873–891.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2016. *A primer on partial least squares structural equation modeling (PLS-SEM)* (Second.), Thousand Oakes: Sage Publications.

Hambrick, D. C., Cho, T. S., and Chen, M. 1996. "The Influence of Top Management Team Heterogeneity on Firms Competitive Moves," *Administrative Science Quarterly* (41:4), pp. 659–684.

Hanneman, R. A., and Riddle, M. 2005. *Introduction to social network methods*, Riverside, CA: University of California (available at http://faculty.ucr.edu/~hanneman/nettext/index.html).

Hau, Y. S., and Kim, Y. G. 2011. "Why would online gamers share their innovation-conducive knowledge in the online game user community? Integrating individual motivations and social capital perspectives," *Computers in Human Behavior* (27:2), pp. 956–970.

Hausken, K. 2015. "A Strategic Analysis of Information Sharing Among Cyber Attackers," *Journal of Information Systems and Technology Management* (12:2), pp. 245–270.

Hausman, J. A. 1978. "Specification tests in econometrics," *Econometrica: Journal of the Econometric* (46:6), pp. 1251–1271.

Henseler, J., Hubona, G., and Ray, P. A. 2016. "Using PLS path modeling in new technology research: updated guidelines," *Industrial Management & Data Systems* (116:1), pp. 2–20 (doi: 10.1108/IMDS-09-2015-0382).

Henseler, J., Ringle, C. M., and Sarstedt, M. 2014. "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 115–135 (doi: 10.1007/s11747-014-0403-8).

Herath, T., and Rao, R. 2009a. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* (47:2), pp. 154–165 (doi: 10.1016/j.dss.2009.02.005).

Herath, T., and Rao, R. 2009b. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), pp. 106–125.

Hinz, O., and Spann, M. 2008. "The impact of information diffusion on bidding behavior in secret reserve price auctions," *Information Systems Research* (19:3), pp. 351–368.

Hippel, E. von, and Krogh, G. von. 2003. "Open Source Software and the 'Private-Collective' Innovation Model: Issues for Organization Science," *Organization Science* (14:2), pp. 209–223.

Ho, S. Y., and Rai, A. 2017. "Continued voluntary participation intention in firm-participating open source software projects," *Information Systems Research* (28:3), pp. 603–625 (doi: 10.1287/isre.2016.0687).

Holmes, J. G. 1991. “Trust and the appraisal process in close relationships.,” in *Advances in Personal Relationships*W. H. Jones and D. Perlman (eds.) (2nd ed.), London, UK: Jessica Kingsley, pp. 57–104.

Holt, T., and Kilger, M. 2008. “Techcrafters and makecrafters: A comparison of two,” in *WOMBAT Workshop on Information Security Threats Data Collect and Sharing*, Amsterdam, Netherlands: IEEE, pp. 67–78.

Holt, T., Strumsky, D., and Smirnova, O. 2012. “Examining the social networks of malware writers and hackers,” *International Journal of Cyber Criminology* (6:1), pp. 891–903.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., and Dhillon, G. 2013. “A framework and guidelines for context-specific theorizing in information systems research,” *Information Systems Research* (25:1), pp. 111–136.

Hosmer, L. T. 1995. “Trust: The connecting link between organizational theory and philosophical ethics,” *Academy of Management Review* (20:2), pp. 379–403.

Hsu, M. K., Jiang, J. J., Klein, G., and Tang, Z. 2003. “Perceived career incentives and intent to leave,” *Information & Management* (40), pp. 361–369 (doi: 10.1146/annurev.publhealth.26.021304.144532).

Ifinedo, P. 2014. “Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,” *Information & Management* (51), pp. 69–79 (doi: 10.1016/j.im.2013.10.001).

Im, I., Jun, J., Oh, W., and Jeong, S.-O. 2016. “Deal-seeking versus brand-seeking: Search behaviors and purchase propensities in sponsored search platforms,” *MIS Quarterly* (40:1), MIS Quarterly, pp. 187–204.

Inkpen, A., and Tsang, T. 2005. “Social capital, networks, and knowledge transfer,” *Academy of Management Review* (30:1), pp. 146–165.

Jackson, M. O. 2008. “Social and Economic Networks,” *Network* (March), pp. 14–16.

Jansen, B. J., Brown, A., and Resnick, M. 2007. “Factors relating to the decision to click on a sponsored link,” *Decision Support Systems* (44:1), pp. 46–59.

Janz, N. K., and Becker, M. H. 1984. “The health belief model: A decade later,” *Health Education & Behavior* (11:1), pp. 1–47.

Jarvis, Cheryl, B., MacKenzie, Scott, B., and Podsakoff, P. M. 2003. “A critical review of construct indicators and measurement model misspecification in marketing and consumer research,” *Journal of consumer research* (30).

Jianakoplos, N., and Bernasek, A. 1998. “Are women more risk averse?,” *Economic Inquiry* (36:4), pp. 1465–7295.

Joachims, T., Granka, L., Pan, B., Hembrooke, H., and Gay, G. 2005. “Accurately interpreting clickthrough data as implicit feedback,” in *Proceedings of the 28th annual international ACM SIGIR conference on Research and development in information retrieval*, ACM, pp. 154–161.

Johnson, S. L., Safadi, H., and Faraj, S. 2015. “The emergence of online community Leadership,” *Information Systems Research* (26:1), pp. 165–187.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. “An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric,” *MIS Quarterly* (39:1), MIS Quarterly, pp. 113-A7.

Jones, M., Mothersbaugh, D., and Beatty, S. E. 2000. “Switching Barries and Repurchase Intentions in Services,” *Journal of Retailing* (76:2), pp. 259–274.

Jordan, T., and Taylor, P. 1998. “A sociology of hackers,” *Sociological Review* (46:4), pp. 757–780.

Kankanhalli, A., Tan, B. C. Y., and Wei, K.-K. 2005. “Contributing knowledge to electronic knowledge repositories: An empirical investigation,” *MIS Quarterly* (29:1), pp. 113–143.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., and Wei, K.-K. 2003. “An integrative study of information systems security effectiveness,” *International Journal of Information Management* (23:2), pp. 139–154.

Kappelman, L., Torres, R., Mclean, E., and Snyder, M. 2017. “SIM IT Trends 2016,” *MIS Quartely Executive* (16:1), pp. 47–80.

Keil, M., Tan, B. C. Y., Wei, K.-K., Saarinen, T., Tuunainen, V., and Wassenaar, A. 2000. “A cross-cultural study on escalation of commitment behavior in software projects,” *MIS Quarterly*, pp. 299–325.

Keller, S., Powell, A., Horstmann, B., Predmore, C., and Crawford, M. 2005. “Information security threats and practices in small businesses,” *Information Systems Management* (22:2), p. 7.

Kennedy, P. 2003. *A guide to econometrics*.

Kettinger, W. J., Zhang, C., and Chang, K. 2013. “A View from the Top : Integrated Information Delivery and Effective Information Use from the Senior Executive ’s Perspective,” *Information Systems Research* (24:3), pp. 842–860.

Khanna, T., Gulati, R., and Nohria, N. 1998. “The dynamics of learning alliances: Competition, cooperation, and relative scope,” *Strategic Management Journal* (19:3), JSTOR, pp. 193–210.

Kierkegaard, P. 2012. “Medical data breaches: Notification delayed is notification denied,” *Computer Law and Security Review* (28:2), Elsevier Ltd, pp. 163–183 (doi: 10.1016/j.clsr.2012.01.003).

Kim, D. J., Ferrin, D. L., and Rao, H. R. 2008. “A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents,” *Decision Support Systems* (44:2), pp. 544–564.

Kim, D. J., Ferrin, D. L., and Rao, H. R. 2009. “Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration,” *Information Systems Research* (20:2), pp. 237–257 (doi: 10.1287/isre.1080.0188).

Kim, S. H., and Kim, B. C. 2014. “Differential Effects of Prior Experience on the Malware Resolution Process,” *MIS Quarterly* (38:3), pp. 655–678.

Kline, R. 1998. *Principles and practice of structural equation modeling*, New York: Guilford Press.

Knapp, K. J., and Boulton, W. R. 2006. “Cyber-warfare threatens corporations: Expansion into commercial environments,” *Information Systems Management* (23:2), p. 76.

Kock, N. 2015. “Common method bias in PLS-SEM: A full collinearity assessment approach,” *International Journal of e-Collaboration* (11:4).

Kock, N., and Gaskins, L. 2014. “The Mediating Role of Voice and Accountability in the Relationship Between Internet Diffusion and Government Corruption in Latin America and Sub-Saharan Africa,” *Information Technology for Development* (20:1), pp. 23–43.

Kock, N., and Lynn, G. 2012. “Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations,” *Journal of the Association for Information Systems* (13:7), pp. 546–580.

Krogh, G. von. 2009. “Individualist and collectivist perspectives on knowledge in organizations: Implications for information systems research,” *Journal of Strategic Information Systems* (18:3), pp. 119–129.

Kwak, Y. H., and LaPlace, K. S. 2005. “Examining risk tolerance in project-driven organization,” *Technovation* (25:6), pp. 691–695 (doi: 10.1016/j.technovation.2003.09.003).

Kwon, J., and Johnson, M. E. 2014. “Proactive versus reactive security investments in the healthcare sector,” *MIS Quarterly* (38:2), pp. 451–471.

Larose, C., and Burke, J. 2015. “CNA Denies Cyber Insurance Claim,” *Privacy and security Matters* (available at https://www.privacyandsecuritymatters.com/2015/05/cna-denies-cyber-insurance-claim/; retrieved January 29, 2018).

Lawsky, B. M. 2014. “New Cyber Security Examination Process,” New York, NY (available at http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf).

Lazarus, R. S., and Smith, C. a. 1988. “Knowledge and Appraisal in the Cognition—Emotion Relationship,” *Cognition & Emotion* (2:4), pp. 281–300.

Lee, Y., and Larsen, K. R. 2009. “Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software,” *European Journal of Information Systems* (18:2), pp. 177–187.

Lewis, W., Agarwal, R., and Sambamurthy, V. 2003. “Sources of influence on beliefs about information technology use: An empirical study of knowledge,” *MIS Quarterly* (27:4), pp. 657–678 (doi: 10.2307/30036552).

Liang, H., and Xue, Y. 2009. “Avoidance of information technology threats: a theoretical perspective,” *MIS Quarterly*, pp. 71–90.

Liang, H., and Xue, Y. 2010. “Understanding security behaviors in personal computer usage: A threat avoidance perspective,” *Journal of the Association for Information*.

Lin, N. 1999. “Building a Network Theory of Social Capital’,” *Connections* (22:1), pp. 28–51.

Lu, Y., Luo, X., Polgar, M., and Cao, Y. 2010. “Social Network Analysis of a Criminal Hacker Community,” *The Journal of Computer Information Systems* (51:2), p. 31.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., and Raghu, T. S. 2010. “Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue.,” *MIS Quarterly* (34:3), pp. 431–433.

Majuca, R. P., Yurcik, W., and Kesan, J. P. 2006. “The Evolution of Cyberinsurance,” (available at http://arxiv.org/ftp/cs/papers/0601/0601020.pdf).

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research* (15:4), pp. 336–355 (doi: doi:10.1287/isre.1040.0032).

Marsh. 2015. “UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk,” (available at https://www.marsh.com/uk/insights/research/uk-cyber-security-role-of-insurance-in-managing-mitigating-risk.html).

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. “An integrative model of organizational trust,” *Academy of Management Review* (20:3), pp. 709–734.

McAfee. 2015. “Netwire RAT Behind Recent Targeted Attacks | McAfee Blogs,” (available at https://securingtomorrow.mcafee.com/mcafee-labs/netwire-rat-behind-recent-targeted-attacks/; retrieved September 1, 2017).

McCarthy, C., Harnett, K., Carter, A., and Hatipoglu, C. 2014. “Assessment of the Information Sharing and Analysis Center Model,” (available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812076-assessinfosharingmodel.pdf).

McKnight, D. H., and Chervany, N. L. 2001. “Conceptualizing trust: A typology and e-commerce customer relationships model,” in *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, IEEE.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. “The impact of initial consumer trust on intentions to transact with a web site: A trust building model,” *Journal of Strategic Information Systems* (11:3–4), pp. 297–323 (doi: 10.1016/S0963-8687(02)00020-3).

McKnight, D. H., Cummings, L. L., and Chervany, N. L. 1998. “Initial trust formation in new organizational relationships,” *Academy of Management Review* (23:3), pp. 473–490.

McKnight, D. H., Phillips, B., and Hardgrave, B. C. 2009. “Which reduces IT turnover intention the most: Workplace characteristics or job characteristics?,” *Information and Management* (46:3), pp. 167–174 (doi: 10.1016/j.im.2009.01.002).

McNicholas, E. 2013. “Cybersecurity Insurance to Mitigate Cyber-Risks and SEC Disclosure Obligations,” *Bloomberg Law* (available at https://www.bna.com/cybersecurity-insurance-to-mitigate-cyber-risks-and-sec-disclosure-obligations/; retrieved January 29, 2018).

Medvinsky, G., Lai, C., and Neuman, B. C. 1994. “Endorsements, licensing, and insurance for distributed system services,” in *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, ACM, pp. 170–175.

Mein Goh, J., Gao, G., and Agarwal, R. 2016. “The Creation of Social Value: Can an Online Health Community Reduce Rural-Urban Health Disparities?,” *MIS Quarterly* (40:1), pp. 247–263.

Meland, P. H., Tondel, I. A., and Solhaug, B. 2015. “Mitigating risk with cyberinsurance,” *IEEE Security and Privacy* (13:6), pp. 38–43 (doi: 10.1109/MSP.2015.137).

Meyer, G. 1989. “The Social Organization of the Computer Underworld,” Northern Ilinois University.

Milne, S., and Orbell, S. 2000. “Can protection motivation theory predict breast selfexamination? A longitudinal test exploring the role of previous behaviour,” *Understanding and changing health behaviour from health beliefs to self-regulation*, pp. 51–71.

Miltgen, C. L., and Smith, H. J. 2015. “Exploring information privacy regulation, risks, trust, and behavior,” *Information and Management* (52:6), Elsevier B.V., pp. 741–759.

Mitchell, V.-W. 1999. “Consumer perceived risk: conceptualisations and models,” *European Journal of marketing* (33:1/2), pp. 163–195.

Mollick, E. 2012. “People and process, suits and innovators: The role of individuals in firm performance,” *Strategic Management Journal* (33:2), pp. 1001–1015 (doi: 10.1002/smj).

Monsma, E., Buskens, V., and Soudijn, M. 2013. “Partners in cybercrime,” *Advances in cyber*.

Mookerjee, V., Mookerjee, R., Bensoussan, A., and Yue, W. T. 2011. “When hackers talk: Managing information security under variable attack rates and knowledge dissemination,” *Information Systems Research* (22:3), pp. 606–623.

Moore, G. C., and Benbasat, I. 1991. “Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation,” *Information Systems Research* (2:3), pp. 192–222.

Moore, J. E. 2000. “One road to turnover: An examination of work exhaustion in technology professionals,” *MIS Quarterly* (24:1), Minneapolis, p. 141.

Moores, T. T., and Chang, J. C.-J. 2006. “Ethical decision making in software piracy: Initial development and test of a four-component model,” *MIS Quarterly*, pp. 167–180.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G. M. 2011. “An analysis of underground forums,” in *ACM SIGCOMM Internet Measurement Conference*, pp. 71–79.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. 2013. “Cyber-risk decision models: To insure IT or not?,” *Decision Support Systems* (56), pp. 11–26.

Naghizadeh, P., and Liu, M. 2016. “Opting Out of Incentive Mechanisms : A Study of Security as a Non-Excludable Public Good,” *IEEE Transactions on Information Forensics and Security* (11:12), pp. 2790–2803.

Nahapiet, J., and Ghoshal, S. 1998. “Social capital, intellectual capital, and the organizational advantage,” *Academy of Management Review* (23:2), pp. 242–266.

NCI. 2016. “How does a data breach affect your business’ reputation?,” (available at http://www.nationalcybersecurityinstitute.org/general-public-interests/how-does-a-data-breach-affect-your-business-reputation/; retrieved September 10, 2016).

Newey, W., and West, K. 1987. “A simple, positive semi-definite, heteroskedasticity and autocorrelation consistent covariance matrix,” *Econometrica* (55:3).

Newman, C., and Stein, D. 2013. “Cyberattacks a Huge Threat to Start-Ups, and Their Investors,” *The New York Times*.

NIST. 2013. “Cybersecurity Framework,” November 12, 2013 (available at http://www.nist.gov/cyberframework/).

Odabas, M., Breiger, R., and Holt, T. 2015. “Toward an Economic Sociology of Online Hacker Communities,” *Twenty-Seventh Annual Meeting*, London, UK: Society for the Advancement of Socio-Economics.

Ogul, M., and Rockman, B. 1990. “Overseeing Oversight: New Departures and Old Problems,” *Legislative Studies Quarterly* (15:1), pp. 5–24.

Öğüt, H., Raghunathan, S., and Menon, N. 2011. “Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection,” *Risk Analysis* (31:3), pp. 497–512.

Oltsik, J. 2015. “The State of Cyber Insurance,” *CSO Online* (available at https://www.csoonline.com/article/3005213/security/the-state-of-cyber-insurance.html; retrieved January 29, 2018).

Panzano, P. C., and Billings, R. S. 1997. “An Organizational-Level Test of a Partially Mediated Model of Risky Decision Making Behavior,” in *Academy of Management Proceedings* (Vol. 1997), Academy of Management, pp. 340–344.

Pavlou, P. A. 2003. “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model,” *International Journal of Electronic Commerce* (7:3), pp. 101–134.

Pavlou, P., and Gefen, D. 2004. “Building effective online marketplaces with institution-based trust,” *Information Systems Research* (15:1), pp. 37–59.

Perkins, H. W., and Craig, D. W. 2006. “A successful social norms campaign to reduce alcohol misuse among college student-athletes.,” *Journal of Studies on Alcohol* (67:November), pp. 880–889 (doi: 10.15288/jsa.2006.67.880).

Peter, J. P., and Tarpey, L. X. 1975. “A comparative analysis of three consumer decision strategies,” *Journal of Consumer Research*, pp. 29–37.

Petkova, A. P., Wadhwa, A., Yao, X., and Jain, S. 2014. “Reputation and Decision Making under Ambiguity : A Study of U . S . Venture Capital Firms ’ Investments in the Emerging Clean Energy Sector,” *Academy of Management Journal* (57:2), pp. 422–448 (doi: 10.5465/amj.2011.0651).

Pew Research. 2015. “Americans’ Internet Access: 2000-2015,” (available at http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/).

Pfleeger, S. L., and Caputo, D. D. 2012. “Leveraging behavioral science to mitigate cyber security risk,” *Computers & Security* (31:4), pp. 597–611.

Pi, S. M., Chou, C. H., and Liao, H. L. 2013. “A study of Facebook Groups members’ knowledge sharing,” *Computers in Human Behavior* (29:5), Elsevier Ltd, pp. 1971–1979 (doi: 10.1016/j.chb.2013.04.019).

Plambeck, N., and Weber, K. 2010. “When the glass is half full and half empty: CEOs’ ambivalent interpretations of strategic issues,” *Strategic Management Journal* (31:7), pp. 689–710.

Png, I. P. L., and Wang, Q.-H. 2009. “Information Security: Facilitating User Precautions Vis-à-Vis Enforcement Against Attackers,” *Journal of Management Information Systems* (26:2), pp. 97–121.

Podolny, J. M., and Baron, J. 1997. “Resources and relationships: Social networks and mobility in the workplace,” *American sociological review* (62:5), pp. 673–693.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *Journal of applied psychology* (88:5), p. 879.

Podsakoff, P. M., MacKenzie, S. B., and Podsakoff, N. P. 2011. "Sources of Method Bias in Social Science Research and Recommendations on How to Control It," *Annual Review of Psychology* (63:1), pp. 539–569.

Ponemon. 2013. "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," Experian (available at http://www.experian.com/innovation/business-resources/ponemon-study-managing-cyber-security-as-business-risk.jsp?ecd_dbres_cyber_insurance_study_ponemon_referral).

Ponemon. 2015a. "Cost of Data Breach," (available at http://www-03.ibm.com/security/data-breach/).

Ponemon. 2015b. "2015 Cost of Cyber Crime Study: United States," (available at http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states).

Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179–214.

Putnam, R. D. 1995. "Bowling Alone: America's Declining Social Capital," *Journal of Democracy*, New York: Palgrave Macmillan US, pp. 65–78.

Quelch, J. A., and Klein, L. R. 1996. "The Internet and international marketing," *Sloan Management Review* (37:3).

Radianti, J. 2010. "A study of a social behavior inside the online black markets," in *International Conference on Emerging Security Information, Systems and Technologies, SECURWARE*, pp. 189–194.

Ransbotham, S., and Mitra, S. 2009. "Choice and chance: A conceptual model of paths to information security compromise," *Information Systems Research* (20:1), pp. 121–139.

Raymond, E. 2000. "How To Become A Hacker," (available at https://people.redhat.com/zaitcev/notes/hacker-howto.html; retrieved January 1, 2016).

Raymond, E. 2001. *The Cathedral & the Bazaar: Musings on linux and open source by an accidental revolutionary*, O'Reilly Media.

Reuters. 2014. "Cyber crime costs global economy $445 billion a year: report," (available at http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609#97FYxHC7fv5UKZsz.97).

Reuters. 2015. "Only 2 percent of large British firms have cyber insurance: report | Reuters.," Rhee, H.-S., Kim, C., and Ryu, Y. U. 2009. "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security* (28:8), pp. 1–11.

Richardson, M., Dominowska, E., and Ragno, R. 2007. "Predicting clicks: Estimating the click-through rate for new Ads," in *Proceedings of the 16th international conference on World Wide Web*, ACM, pp. 521–530.

Rindova, V., Pollock, T., and Hayward, M. 2006. "Celebrity firms: The social construction of market popularity," *Academy of management* (32:1), pp. 50–71.

Ringle, C. M., Wende, S., and Will, A. 2005. "SmartPLS 2.0," Hamburg, Germany.

Samtani, S. 2016. "Hacker Web Forum Collection: Hackhound Forum Dataset," University of Arizona Artificial Intelligence Lab, AZSecure-data, Director Hsinchun Chen (available at http://www.azsecure-data.org/; retrieved June 3, 2016).

Santos, F., and Eisenhardt, K. 2009. "Constructing markets and shaping boundaries: Entrepreneurial power in nascent fields," *Academy of Management Journal* (52:4), pp. 643–671.

Sarma, M., and Lam, A. 2013. "Knowledge creation and innovation in the virtual community? Exploring structure, values and identity in hacker groups," in *35th DRUID Celebration Conference*, Barcelona, Spain.

Sasse, M. A., and Kirlappos, I. 2011. "Familiarity breeds con-victims: why we need more effective trust signaling," in *Trust Management V*, Springer, pp. 9–12.

Schneier, B. 2001. "Insurance and the computer industry," *Communications of the ACM* (44:3), pp. 114–115.

SEC. 2011. "SEC CF Disclosure Guidance: Cybersecurity," *SEC* (available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm; retrieved January 29, 2018).

Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314–341 (doi: 10.1080/07421222.2015.1063315).

Siegel, C. A., Sagalow, T. R., and Serritella, P. 2002. "Cyber-risk management: technical and insurance controls for enterprise-level security," *Information Systems Security* (11:4), pp. 33–49.

Siponen, M., and Vance, A. 2010. "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly* (34:3), p. 487.

Sitkin, S. B., and Pablo, A. L. 1992. "Reconceptualizing the determinants of risk behavior," *Academy of management review* (17:1), pp. 9–38.

Sitkin, S. B., and Weingart, L. R. 1995. “Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity,” *Academy of Management Journal* (38:6), pp. 1573–1592.

Sloof, R., and van Praag, C. M. 2008. “Performance measurement, expectancy and agency theory: An experimental study,” *Journal of Economic Behavior and Organization* (67:3–4), pp. 794–809 (doi: 10.1016/j.jebo.2007.09.003).

Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. J. 2006. “Concern for information privacy and online consumer purchasing,” *Journal of the Association for Information Systems* (7:1), p. 16.

Smith, H. J., Dinev, T., and Xu, H. 2011. “Information privacy research: an interdisciplinary review,” *MIS Quarterly* (35:4), pp. 989–1016.

Spears, J. L., and Barki, H. 2010. “User participation in information systems security risk management,” *MIS Quarterly* (34:3), pp. 503–522.

Sproull, L., and Arriaga, M. 2007. “Online communities,” in *Handbook of Computer Networks*H. Bidogli (ed.), New York: John Wiley & Sons.

Srinidhi, B., Yan, J., and Tayi, G. K. 2015. “Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors,” *Decision Support Systems* (75), pp. 49–62.

Staiger, D., and Stock, J. 1997. “Instrumental variables regression with weak instruments,” *Econometrica: Journal of the Econometric Society* (65:3), pp. 557–586.

Stewart, and Daniel. 2005. “Social Status in an Open-Source Community,” *American Sociological Review* (70:5), pp. 824–842.

Stone, M. 1974. “Cross-validatory choice and assessment of statistical predictions,” *Journal of the Royal Statistical Society* (36:2), pp. 111–147.

Straub, D. W., and Ang, S. 2008. “Editor’s comments: Readability and the relevance versus rigor debate,” *MIS Quarterly*, pp. iii–xiii.

Straub, D. W., and Welke, R. J. 1998. “Coping with systems risk: security planning models for management decision making,” *MIS Quarterly*, pp. 441–469.

Sunden, A., and Surette, B. 1998. “Gender differences in the allocation of assets in retirement savings plans,” *The American Economic Review* (88:2), pp. 207–211.

Symantec. 2006. “Severity Assessment: Threats, events, vulnerabilities, risks,” (available at https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Severity-Assesment.pdf).

Symantec. 2014. “Internet Security Threat Report 2014,” (available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf).

Thomas, D. 2002. *Hacker culture*, Minneapolis, MN: University of Minnesota Press.

Thomas, J. 2005. “The moral ambiguity of social control in cyberspace: a retro-assessment of the ‘golden age’ of hacking,” *New Media & Society* (7:5), pp. 599–624.

Tiwana, A. 2003. “Knowledge Partitioning in Outsourced Software Development: A Field Study,” in *ICIS 2003 Proceedings*, pp. 259–270.

Trevino, L. K. 1992. “Experimental approaches to studying ethical-unethical behavior in organizations,” *Business Ethics Quarterly* (2:3), pp. 121–136.

Trier, M. 2008. “Towards dynamic visualization for understanding evolution of digital communication networks,” *Information Systems Research* (19:3), pp. 335–350.

Tsai, W. 2002. “Social Structure of ‘Coopetition’ Within a Multiunit Organization: Coordination, Competition, and Intraorganizational Knowledge Sharing,” *Organization Science* (13:2), pp. 179–190.

Tushman, M. 1977. “Special boundary roles in the innovation process,” *Administrative science quarterly* (22:4), pp. 587–605.

Vance, A., Siponen, M., and Pahnila, S. 2012a. “Motivating IS security compliance: Insights from habit and protection motivation theory,” *Information & Management* (49:3), pp. 190–198.

Vance, A., Siponen, M., and Pahnila, S. 2012b. “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Information & Management* (49:3–4), pp. 190–198 (available at http://www.sciencedirect.com/science/article/pii/S0378720612000328).

Venkatesh, V., and Agarwal, R. 2006. “Turning visitors into customers: a usability-centric perspective on purchase behavior in electronic channels,” *Management Science* (52:3), pp. 367–382.

Venkatesh, V., Morris, M. G., Gordon, B. D., and Davis, F. D. 2003. “User Acceptance of Information Technology: Toward a Unified View,” *MIS Quarterly* (27:3), Management Information Systems Research Center, University of Minnesota, pp. 425–478 (doi: 10.2307/30036540).

Wall Street Journal, The. 2012. “Cybercriminals Sniff Out Vulnerable Firms,” (available at https://www.wsj.com/articles/SB10001424052702303933404577504790964060610; retrieved January 1, 2017).

Wang, J., Li, Y., and Rao, H. R. 2017. “Coping responses in phishing detection: An investigation of antecedents and consequences,” *Information Systems Research* (28:2), pp. 378–396 (doi: 10.1287/isre.2016.0680).

Wang, S., and Noe, R. 2010. “Knowledge sharing: A review and directions for future research,” *Human Resource Management Review*.

Wang, T., Kannan, K. N., Ulmer, J. R., Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. “The Association Between the Disclosure and the Realization of Information Security Risk Factors The Association Between the Disclosure and the Realization of Information Security Risk Factors,” *Information Systems Research* (May 2016).

Warkentin, M., Goel, S., and Menard, P. 2017. “Shared Benefits and Information Privacy : What Determines Smart Meter Technology Adoption ? Abstract,” *Journal of the Association for Information Systems* (18:11), pp. 758–786.

Wasko, M., and 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*.

Wasko, M. W., and Faraj, S. 2005. “Why Should I Share? Examining Social Capital and Knowledge Contribution in Electronic Networks of Practice,” *MIS Quarterly* (29:1).

Wasserman, S., and Faust, K. 1994. *Social network analysis: Methods and applications*.

Wattal, S., and Telang, R. 2004. “Effect of Vulnerability Disclosures on Market Value of Software Vendors–An Event Study Analysis.,”

Weaver, G. R., Trevino, L. K., and Cochran, P. L. 1999. “Corporate ethics programs as control systems: influences of excecutive commitment and environmental factors,” *Academy of Management Journal* (42:1), pp. 41–57 (doi: 10.2307/256873).

Weber, J. 1992. “Scenarios in business ethics research: Review, critical assessment, and recommendations,” *Business Ethics Quarterly* (2:2), pp. 137–160.

Webster, J., and Trevino, L. K. 1995. “Rational and social theories as complementary explanations of communication media choices: Two policy-capturing studies,” *Academy of Management Journal* (38:6), pp. 1544–1572.

Whetten, D. A. 1989. “What constitutes a theoretical contribution?,” *Academy of management review* (14:4), pp. 490–495.

White, H. 1980. “A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity,” *Econometrica: Journal of the Econometric Society* (48:4), pp. 817–838.

Willison, R., and Warkentin, M. 2013. “Beyond deterrence: An expanded view of employee computer abuse,” *MIS Quarterly* (37:1), pp. 1–20 (doi: 10.1080/01639625.2012.759048).

Wolfinbarger, M., and Gilly, M. C. 2001. “Shopping online for freedom, control, and fun,” *California Management Review* (43:2), pp. 34–55.

Workman, M. 2007. “Gaining access with social engineering: An empirical study of the threat,” *Information Systems Security* (16:6), Taylor & Francis, pp. 315–331.

Xia, M., Huang, Y., Duan, W., and Whinston, A. B. 2012. “Research Note — To Continue Sharing or Not to Continue Peer Sharing Networks To Continue Sharing or Not to Continue Sharing ? An Empirical Analysis of User Decision in Peer-to-Peer Sharing Networks,” *Information Systems Research* (23:1), pp. 247–259 (doi: 10.1287/isre.1100.0344).

Yan, Z., Wang, T., Chen, Y., and Zhang, H. 2016. “Knowledge sharing in online health communities: A social exchange theory perspective,” *Information & Management* (53:5), pp. 643–653.

Yaraghi, N., Du, A. Y., Sharman, R., Gopal, R. D., and Ramesh, R. 2015. “Health Information Exchange as a Multisided Platform: Adoption, Usage and Practice Involvement in Services Co-Production,” *Information Systems Research* (26:1), pp. 1–18.

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

Young, D., Lopez, J., Rice, M., Ramsey, B., and McTasney, R. 2016. “A framework for incorporating insurance in critical infrastructure cyber risk strategies,” *International Journal of Critical Infrastructure Protection* (14), pp. 43–57 (doi: 10.1016/j.ijcip.2016.04.001).

Young, R., Zhang, L., and Prybutok, V. R. 2007. “Hacking into the Minds of Hackers,” *Information Systems Management* (24:4), pp. 281–287.

Yuwei, L. 2005. “The Future of Sociology of FLOSS,” *First Monday* (2).

Zahedi, F. " M., and Song, J. 2008. “Dynamics of trust revision: Using health infomediaries,” *Journal of Management Information Systems* (24:4), pp. 225–248.

Zhang, X., Guo, X., Wu, Y., Lai, K.-H., and Vogel, D. 2017. “Exploring the inhibitors of online health service use intention: a status quo bias perspective,” *Information & Management* (doi: 10.1016/j.im.2017.02.001).

Zhang, X., Tsang, A., Yue, W. T., and Chau, M. 2015. “The classification of hackers by knowledge exchange behaviors,” *Information Systems Frontiers* (17:6), pp. 1239–1251.

Zhao, X., Xue, L., and Whinston, A. B. 2013. “Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements,” *Journal of Management Information Systems* (30:1), pp. 123–152.

Zhou, T., Lu, Y., and Wang, B. 2009. “The relative importance of website design quality and service quality in determining consumers’ online repurchase behavior,” *Information Systems Management* (26:4), pp. 327–337.

Ziobro, P., and Lublin, J. 2014. “ISS’s View on Target Directors Is a Signal on Cybersecurity,” *The Wall Street Journal* (available at https://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278; retrieved January 30, 2018).