THE IMPACT OF INFORMATION SECURITY AWARENESS ON COMPLIANCE WITH INFORMATION SECURITY POLICIES: A PHISHING PERSPECTIVE

Bartlomiej T. Hanus

Dissertation Prepared for the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

August 2014

APPROVED:

John Windsor, Major Professor
Robert Pavur, Committee Member
Dan J. Kim, Committee Member
Andy Wu, Committee Member
Mary Jones, Chair of the Department of
    Information Technology and Decision
    Sciences
O. Finley Graves, Dean of the College of
    Business
Mark Wardell, Dean of the Toulouse Graduate
    School

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Hanus, Bartlomiej T. The Impact of Information Security Awareness on Compliance with Information Security Policies: A Phishing Perspective. Doctor of Philosophy (Business Computer Information Systems), August 2014, 153 pp., 23 tables, 4 figures, references, 161 titles.

This research seeks to derive and examine a multidimensional definition of information security awareness, investigate its antecedents, and analyze its effects on compliance with organizational information security policies. The above research goals are tested through the theoretical lens of technology threat avoidance theory and protection motivation theory. Information security awareness is defined as a second-order construct composed of the elements of threat and coping appraisals supplemented by the responsibilities construct to account for organizational environment.

The study is executed in two stages. First, the participants (employees of a municipality) are exposed to a series of phishing and spear-phishing messages to assess if there are any common characteristics shared by the phishing victims. The differences between the phished and the not phished group are assessed through multiple discriminant analysis. Second, the same individuals are asked to participate in a survey designed to examine their security awareness. The research model is tested using PLS-SEM approach.

The results indicate that security awareness is in fact a second-order formative construct composed of six components. There are significant differences in security awareness levels between the victims of the phishing experiment and the employees who maintain compliance with security policies. The study extends the theory by proposing and validating a universal definition of security awareness. It provides practitioners with an instrument to examine awareness in a plethora of settings and design customized security training activities.

ACKNOWLEDGEMENTS

I would like to thank my committee, Dr. Windsor, Dr. Pavur, Dr. Kim, and Dr. Wu for the guidance and patience they have demonstrated during the dissertation process. I would also like to thank all my friends thanks to whom I never felt alone during my PhD studies. Finally, I would like to thank my family for all their unconditional support.

I would like to dedicate this work to my Mom.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Information is central to the functioning of modern day organizations. More specifically, information is the primary factor that holds organizations together (Stamper, 1973). Based on the above, we can define organizations as entities and relationships joined together by the flow of information. This centrality ultimately imposes critical value to information, and the processes related to acquiring, processing and maintaining it. Safeguarding information in organizations is the responsibility of information security, which is an important area of information systems that carries several important functions in organizations, including: protection of organization's ability to function, assurance of safe operations of the organization's information technology (IT) infrastructure, and protection of organizational data, information, and other assets (Whitman & Mattord, 2012). The above is generally known as the mission of information security, based on which a broad definition of information system security can be derived as the state of being free from danger, and at the same time, not exposed to potential damage from attacks or accidents. Information security can also be defined as a process for achieving the above state. Thus, the main objective of any given organization implementing information security is to augment the performance of such organizations with regards to risk exposure and avoidance (Bosworth & Jacobson, 2002).

From a practical perspective, an abundance of obstacles to information security can be identified. First and foremost, security is often perceived as a form of "necessary evil" and an inconvenience. On one end of the spectrum, there are people – members of organizations trying to perform their everyday routines; on the other end – there are security measures that more often than not impose obstacles to human productivity (i.e., passwords and/or other forms of authentication, etc.). Consequently, any time devoted to security compliance occurs at the expense of productivity. Second, information systems are complex and regular users are not necessarily familiar with the information technology aspects of IS. Moreover, computers have been designed as a type of positive technology, while information security exemplifies a protective aspect of it (Dinev & Hu, 2007). Third, current trends in information systems favor information sharing and collaboration between and across users that are often geographically and temporally dispersed from each other (O'Leary & Cummings, 2007) – a situation which is amplified even more through the phenomenon of ubiquitous computing coming to fruition. As a result, information is accessible from plethora of devices connected to heterogeneous media, and this trend will continue on through the convergence of several technologies: increased reliance on cloud computing services, the adoption of social media in organizations, big data solutions, and mobile device adoption (e.g., "bring your own device" – BYOD initiatives, etc.). At the same time, organizations often fail to realize that information security is not only about hardware and software. Humans are part of information systems as well. As reality often reveals – humans are the weakest link in information security (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). Coincidentally, the increased usage of new technologies and the persistence of human weakness in security offer new opportunities for cyber criminals. According to Deloitte's Global Security Survey, the top information security threats for 2012 include threats related to adoption of the aforementioned emerging technologies in organizations (i.e., cloud computing, mobile devices), as well as threats persistently related to human factors (i.e., employee errors and omissions, employee abuse of information systems)

(Deloitte, 2012). In similar fashion, other industry experts also agree that information security threats related to human factors remain an unsolved issue for most enterprises (Sophos Group, 2012). Moreover, the threats related to human behavior have not changed too much in the recent years in comparison to what they used to be (Whitman, 2003). These threats are generally exemplified by the increased focus on spear-phishing and social engineering, and cyber espionage. More specifically, top exploitable human vulnerabilities that continue to pose a risk to security include: lack of awareness, phishability, password reuse, using unpatched and poorly configured BYOD devices, indiscriminate use of mobile media, data leakage via social networking, and accidental disclosure or loss of information/equipment (Spitzner, 2013).

In order to successfully implement security, organizations should follow a well-structured plan. One of the most important aspects of any information security implementation is to accurately address the requirement for proper security training for employees and the development of a security culture within an organization (Mallery, 2009), as well maintaining situational awareness of information security threats (Department of Homeland Security, 2013). This need is often holistically referred to as security, education, training, and awareness (SETA) program, and its purpose is to improve awareness and develop skills and knowledge related to information security (National Institute of Standards and Technology, 2003).

SETA programs are important for several reasons that include: regulatory compliance, customer trust and satisfaction, compliance with internal information security policies, due diligence, corporate reputation, and accountability to name a few of the most important ones (Herold, 2010). The current practitioner-oriented literature strongly emphasizes the need for building information security awareness, especially if we consider the prevalent existence of security threats resulting from human vulnerabilities and ravening presence of cyber criminals with strong intent of exploitation of such weaknesses in organizational defenses.

From academic perspective, the lack of information security awareness has also been broadly discussed by scholars, indicating that there are still unresolved issues in that area of knowledge. It has been determined that security awareness is a significant factor determining compliance with information security policies. However, current literature on security awareness does not address this topic to the full extent of possibilities. In particular, the multidimensionality aspect of information security awareness is a topic that is heavily underrepresented and underexplored in the current body of knowledge. There is a significant gap in research in terms of in-depth identification of dimensions and elements of information security awareness (Dinev & Hu, 2007), as well as the antecedents of thereof (Bulgurcu, Cavusoglu, & Benbasat, 2010). Moreover, present research on security awareness often refers only to the relationships between security awareness and behavioral intentions, indicating the need for studies examining the relationship between the former and the actual information security-related behaviors (e.g., compliance with information security policies) (D’Arcy, Hovav, & Galletta, 2009; Herath & Rao, 2009b).

Drawing on well-established theoretical frameworks – protection motivation theory (PMT) (Maddux & Rogers, 1983; Rogers, 1975) and technology threat avoidance theory (TTAT) (Liang & Xue, 2009), this study addresses the above research gaps by proposing a multidimensional model of information security awareness, identifying the antecedents of security awareness, and measuring the impact of awareness on compliance (i.e., the actual behavior) with information security policies in an organization. This study conceptualizes information security awareness as a state of knowledge composed of several dimensions relevant to assessment and coping with information security threats (i.e., threat definition, recognition, avoidance, potential threat effect, and individual's responsibilities with regards to threats). At the same time, the multidimensional concept of security awareness is conceptualized through the introduction of TTAT, a theory which explains individuals' behaviors of avoiding security threats. The dimensions of security awareness defined in this study are operationalized through threat and coping appraisals defined in TTAT and PMT, thus capturing the multidimensionality aspect of the problem under investigation; as well as coping behaviors represented in this study in the form of compliance with information security policies.

The primary goals of this study are to: (1) examine the multidimensional nature of information security awareness and its relationship with security policy compliance, (2) identify the antecedents of security awareness, and (3) examine actual human behavior in addition to traditionally measured behavioral intention. The study investigates the following research questions. What are the dimensions of information security awareness? What are the antecedents of security awareness? Are there significant differences between individuals who demonstrate behaviors compliant with information security policies and those who do not? What are the key determinants of compliance with security policies?

The contribution of this study is threefold. First, it extends the academic body of knowledge on information security awareness by providing a multidimensional definition of the construct, and thus offering a direct solution that integrates the different approaches found in the current body of knowledge. Second, the study investigates the antecedents of security awareness conceptualized through environmental and intrapersonal factors, which will provide scholars with extended theoretical frameworks for investigating the issue in the future. Third, the proposed definition of security awareness bridges the gap between theoretical rigor and practical relevance by offering a tool that evaluates security awareness that is based on sound theoretical foundations. At the same time, the instrument is readily available to be implemented across a plethora of settings. In addition, the proposed instrument allows for direct comparison of the results with other studies through the implementation of multigroup analysis method, which in turn addresses the issue of generalizability of results.

CHAPTER 2

LITERATURE REVIEW

Current research on information security awareness can be divided into two major streams that to some extent complement each other, and are often used in a combination to deliver a more exhaustive explanation of the phenomenon. Hence, on one hand, there are theoretical approaches deeply rooted in criminological theories. That side of research is predominantly (but not exclusively) represented by general deterrence theory (GDT) (Straub & Welke, 1998). On the other hand, a vast number of psychological theories have been implemented to study the area of information security as well, most often through theory of reasoned action (TRA), theory of planned behavior (TPB), and protection motivation theory (PMT). In the following paragraphs each of the two research streams are discussed (along with underlying theoretical assumptions), and summarized findings and contributions of each stream are presented. Since majority of studies are grounded in either GDT or PMT, these two theories will serve as a backbone for the discussion on up-to-date research on information security, with other frameworks mentioned as necessary. Based on the literature review, the gaps in present research are identified followed by the development of the research goals for this study. Next, the theoretical development of security awareness construct is presented. Finally, theoretical framework for this study is presented, followed by the development of the research model and corresponding hypotheses.

Criminological Theories

Criminology is an area of science that is focused on knowledge of crime and delinquency as social phenomena. Its scope is fairly broad, as it includes all activities related to making laws, breaking laws, and reacting to the breaking of laws (Sutherland, Cressey, & Luckenbill, 1992). Classical and positivist philosophies are the two most widely known schools of thought in criminology. The classical movement proposed that crime was an act of free will. According to this stream, those who commit crimes, commit them in the spirit of free choice and free will. Such individuals would weigh the consequences of their subsequent actions. This rather hedonistic approach assumes that people would seek pleasure and avoid pain. The ultimate judgment on whether to commit a crime would be the result of evaluation of costs and benefits associated with such action. On the other hand, positivist school of thought in criminology attempts to explain criminal behavior as being heavily influenced by the external world. That is, it assumes that human behavior is ultimately determined by biological, psychological, and social factors. Early criminological theories that evolved from the positivist thinking did not withstand the test of time, as they could be perceived as discriminatory in nature. For example, one of the most widely known example is the Lombroso's theory (Lombroso, 1911) which suggests that some individuals bear particular hereditary or atavistic traits that cause them to commit crimes more often that those individuals that do not have such traits. The estimation of validity of such theories is left to the reader, yet, they deserve mentioning to illustrate the differences between both classical and positivist approaches to criminology, by showing where such philosophies have originated from. Those two schools of thought have vastly influenced the theories that followed within each stream. Criminological theories deserve a separate discussion because they delineate abusive, anti-social behaviors from the whole set of noncompliant and undesired behaviors. The criteria for such distinction is simple, such behaviors indicate that a given individual possibly understands that some forms of behaviors will not be considered adherent to be suitable by the current social surrounding, yet she consciously decides to execute certain actions anyway. This phenomenon is sometimes operationalized as the insider's threat (Warkentin & Willison, 2009; Willison & Warkentin, 2013). On the other hand, the remainder of noncompliant behaviors may be unintentional and caused by the lack of proper levels of awareness and knowledge, presence of which could entirely reverse the judgments of such people.

GDT is an example of a classical theory. It has evolved from rational choice theory that laid the foundation for this school of thought. It implies that human choices are based on certain rationale, a calculation as some may claim. The choice between conformance and or deviance is a direct result of basic cost-benefit analysis. Deterrence theory introduces the concept of punishment and evaluates its impact within the three major dimensions: severity, certainty, and celerity (vel swiftness) (Ball, Lilly, & Cullen, 2010). Within the realm of information security, Straub (1990) has introduced GDT to determine the effectiveness of IS security deterrents on diminishing the magnitude of computer abuse. Deterrence in terms of information security focuses on sanctions which are represented by the certainty (i.e., risk of punishment) and severity (i.e., strictness of penalties) of sanctions. While information security awareness is not explicitly addressed, Straub is rather focusing on the fact of making individuals aware of the efforts to control anti-social behaviors. In terms of information security, deterrents are classified as either of the following: the general security efforts, dissemination of information about potential penalties related to abusive behaviors, promoting acceptable system use through various guidelines, and implementation security policies that describe what is considered to be an acceptable behavior with regards to computer use. Interestingly, Straub offers other (than deterrents) factors the can significantly impact abusive behaviors, which include the use of preventive security software, motivational elements that decrease the likelihood of abuse, and environmental factors affecting misbehaviors. Such classification is extremely confusing, because, for example, the use of preventive security software (and hardware as well, to be more specific) is deterrent itself, and it should be discussed as a separate factor. Moreover, the usage of security infrastructure (both hardware and software) could easily serve as an extension of organizational security policy, and enforce the policy's prescriptions on users in an automated manner. Thus, any intentions of exercising abusive behaviors would be deterred by hardware and software solutions, and would require effortful attempts to circumvent such safeguards. What is more, those types of deterrents could additionally serve as both reinforcements of security awareness by notifying users of what is considered desired behaviors, and as instruments that potentially affect individuals' motivation as well. This study takes a different approach and argues that Straub's approach does not reflect the complexity of building information security awareness. Nevertheless, the results emphasize the importance of having a well-designed security policy in place, and the importance of training and education. In similar fashion, Straub and Welke (1998) treat security awareness as one of possible deterrent countermeasures that organizations can employ to raise the levels of knowledge about information security among its employees and other stakeholders. More importantly, Straub and Welke's understanding of security awareness involves not only knowledge about sanctions, but also knowledge about threats and vulnerabilities. Still, the major premise of security awareness programs is to communicate the information about the central factors of GDT: severity and certainty of sanctions. It could be argued that such an approach is not the sole purpose of awareness programs. And even if it is, then one should ask himself which of the following is a more desirable outcome of security awareness initiatives: threatening individuals with severe punishments or educating them about threats and respective countermeasures? Yet, Straub and Welke emphasize that lack of security awareness should be a serious concern for both individuals and organizations. The literature on the topic considers security awareness to be the most cost-effective measure that in the long-term will lead to higher compliance with security policies (Dhillon, 1999).

A more comprehensive approach to GDT is presented by D'Arcy et al. (2009), who extend the Straub's (1990) original GDT model. It is emphasized that security policies provide knowledge of what is considered acceptable behavior and what constitutes unacceptable conduct with regards to information security, as such policies clearly provide explicit information about the consequences of noncompliance (i.e., punishment) (J. Lee & Lee, 2002). D'Arcy's et al. explicate the context of GDT by suggesting that user awareness of security countermeasures (i.e., security policies, SETA programs, and computer monitoring) has a significant impact on severity and certainty of sanctions. Fundamentally, such an approach integrates original work of Straub, but it does not offer conclusive evidence on the impact of deterrents on shaping individual behavior. Awareness of all three countermeasures has a significant impact on individuals' perceptions of severity and certainty of sanctions. However, the results also suggest that only severe punishment can significantly affect individuals' judgments. When the punishment is certain, but not severe then it is likely that some individuals will decide not to conform to socially accepted behaviors with regards to information systems security. Therefore, the applicability of GDT only in order to study information security awareness and compliant behaviors remains questionable, as the literature on the topic does not provide conclusive evidence on the effectiveness of the sanction/reward model. Some studies report significant results (Gopal & Sanders, 1997; Kankanhalli, Teo, Tan, & Wei, 2003), while others offer inconclusive evidence (D'Arcy et al., 2009; S. M. Lee, Lee, & Yoo, 2004), or even an inverse relationship between severity of sanctions and behaviors (Herath & Rao, 2009a, 2009b). An alternative solution is proposed by Siponen and Vance (2010), who suggest that another criminological theory – neutralization theory may be more useful in explaining violations of information security policies.

A more comprehensive methodology is suggested by Lee and Lee (2002), who offer a holistic approach towards security compliance. They still remain within the area of criminological theories. However, their study integrates both classical and positivist approach from criminology; GDT elements are combined with social bond theory (SBT) (Hirschi, 2002) and social learning theory (SLT) (Akers, Krohn, Lanza-Kaduce, & Radosevich, 1979). SBT involves external factors that could affect individuals' delinquent behaviors, which include the following: attachment to others, commitment to a particular lifestyle, involvement in generally accepted values, and beliefs about the correctness of rules recognized as appropriate by the society. According to this theory, all people are predestined to commit crimes, unless there is a social bond – the relationship that the individual has with the society – that prevents them from doing so. In other words, the stronger the bond, the less likely the individual is to engage in socially unacceptable behaviors. On the other hand, however, the case of what is considered acceptable and unacceptable strongly depends on a given individual's social background. Various social groups do not necessarily have to share the same values. Hence, what might be considered socially unacceptable in a workplace might have an entirely different meaning in the individual's family, neighborhood, religious group, etc. From the security awareness perspective, it is absolutely essential to recognize such differences, and make certain that such differences will be addressed by the proper security training. At the same time, the policy makers need to recognize the fact that the aforementioned human bonds may not be easy to change within a short period of time. Consequently, the decision makers need to remember that SETA programs are ongoing, continuous efforts. SLT is somewhat similar to SBT. It assumes that criminal behaviors are learned through interaction with criminal elements. Such connections could be sometimes approving of delinquent behaviors, or justify them under certain conditions. This phenomenon is known as the differential association (Sutherland et al., 1992), however, it is beyond the scope of present study.

To conclude the discussion on criminological theories, no matter whether GDT is employed alone (D'Arcy et al., 2009; D'Arcy & Hovav, 2007, 2009; Straub & Welke, 1998) or in conjunction with other theoretical frameworks (Bulgurcu et al., 2010; Herath & Rao, 2009b; Pahnila, Siponen, & Mahmood, 2007; Siponen & Vance, 2010), they all emphasize the importance of sanctions (i.e., severity and certainty) on individuals' subsequent actions.

Psychological Theories

The next area of research on information security awareness combines a vast array of psychological theories, occasionally with parts of criminological theories, but more often intermingling instances of the former theories together. As the results of those studies often reveal, such attempts are fully justified, since information security awareness is complex in nature and should not be pigeonholed within one narrow framework. Furthermore, research on security awareness or even on information security per se, is still in its infancy comparing to other areas of the information systems discipline. Thus, researchers are still seeking a broad promiscuous theoretical framework that would allow scholars to fully capture all of the significant nuances of this exciting phenomenon. This review will take the following approach to such mixed-theory studies: (1) discuss the underlying theories, (2) present the approach towards the definition and meaning of information security awareness, (3) present the approach towards compliance, and (4) discuss the importance of SETA programs when available.

Studies that are based on protection motivation theory (PMT) (Rogers, 1975, 1983) represent a significant part of research on information security. In essence, PMT discusses the motivational rationale that lies behind individuals' response to stressful situations, extending the work of Lazarus (Lazarus & Folkman, 1984). PMT describes behaviors associated with coping with health threats. Such behaviors result from two appraisal processes – threat appraisal and coping appraisal, in which individuals weigh the options that could potentially diminish the perceived threat. The sum of both processes results in the intention to perform adaptive responses (i.e., protection motivation) or may lead to maladaptive responses. Maladaptive responses are those that place an individual at risk and consist of behaviors that lead to negative consequences, or the lack of behaviors that eventually may lead to negative consequences. Threat appraisal includes perceived severity and perceived vulnerability. The former refers to the magnitude of a threat that a given event could involve. The latter is associated with the probability of the event actually occurring. At the same time, coping appraisal involves response efficacy, self-efficacy, and the perceived cost of a response.

Response efficacy refers to the effectiveness of recommended behaviors. Self-efficacy describes the degree to which a given individual believes that he could implement the recommended protective behavior. Finally, response cost is associated with different types of costs entailed in the recommended behaviors (e.g., cognitive effort, time, financial cost, etc.). The detailed discussion on PMT application in the area of information security is necessary because the tenets of protection motivation directly relate to the concept of information security awareness.

PMT has been applied in various settings in order to study security-related behavior in IS. Generally, the findings from several studies are consistent to an extent; however, it appears that the overall results are often context dependent. Thus, the generalization of the explanatory power of PMT should be attempted with caution. PMT has been applied to study behaviors either within individuals' personal environment or in workplace. While the behaviors might differ significantly between the two, for example because of social norms and bonds (J. Lee & Lee, 2002), it should be emphasized that both environments are interrelated. It should be also remembered that motivational factors may differ between the two environments (i.e., voluntary vs. mandatory).

From personal environment perspective, Crossler (2010) investigates the backup of files on individuals' personal computer. His results show that both self-efficacy and response efficacy have a significant positive influence on the process of backing up data. However, the costs of preventive actions are not significant predictors of the recommended behaviors. At the same time, variables related to the threat appraisal side of protection motivation have a negative influence on this type of behavior. Continuing with the home setting stream of PMT research, Woon et al. (2005) study the implementation of security features on wireless home network. Similar to Crossler's findings, Woon et al. report that all elements that form coping appraisal (i.e., self-efficacy, response efficacy, and response cost) have a significant positive relationship with recommended behaviors related to having security features enabled on home Wi-Fi networks. Contrary to Crossler's results, perceived severity also has a positive significant influence on behaviors, while it appears that people are not necessarily aware of security risks associated with wireless networking. Again, these results should be treated with care – the study was published almost nine years ago when wireless networking was not as common as it is nowadays. Thus, the risks associated with the technology may have not been widely known to the general public. Still, these inconsistent results provide invaluable insight on the nature of the phenomenon – it appears that the majority of people may be slightly over-confident about their own information security skills. However, that optimism may be caused by the fact that the detailed knowledge of what information security threats are is simply not present. Unlike individuals who are subjected to corporate SETA programs, at least some home users had never been exposed to any sort of information security training. In addition, they do not necessarily receive the same level of technical protection and technical support from IS professionals as corporate users do (Anderson & Agarwal, 2010). Consequently, the lack of knowledge about such threats could significantly affect the perceptions of the potential effects (perceived severity) and the estimation of the likelihood of being exposed to them (perceived vulnerability). Furthermore, this lack of comprehensive understanding of the nature of various threats can also lead to misinterpretation of response costs associated with adaptive behaviors (vide inconclusive results of the above studies). This line if thinking is one the main assumptions of the present research – it is argues that information security awareness is actually a multidimensional construct, with different elements affecting each other. It also remains an open question on how to effectively educate home users (LaRose, Rifon, & Enbody, 2008), the answer to which lies outside of the scope of this research project. Still, assuming the existence of transference of knowledge between work and home environments, partial responsibility could be assigned to organizations, hoping that at least some of the information security practices learned at work will also be employed outside of the workplace.

From the organizational perspective, PMT applications in security are much more widely represented in the literature. The elements of protection motivation are ultimately related to compliance with organizational information security policies. For example, Siponen, Pahnila, and Mahmood (2006) find that, both threat and coping appraisals have significant influence on behavioral intention to comply with information security policies. Additionally, the former is significantly affected by normative beliefs (i.e., potentially persuasive expectations of others) and visibility (i.e., seeing other people use a system or technology). These findings are in line with the conclusions drawn from studying PMT in home settings. That is, within a corporate environment users may be exposed not only to training, but also to persuasion and cooperation with other people. Thus, their actual awareness of security threats may be higher due to the fact that they may be exposed to a more comprehensive perspective of information security threats. This findings are confirmed by the same authors (Pahnila et al., 2007) in a broader study, which additionally yields that neither sanctions nor rewards have significant impact on intention to comply, and actual compliance with security policies respectively. Furthermore, it also appears that organizational involvement into raising information security awareness is in important factor for achieving security policy compliance, which is depicted by the significant impact of facilitating conditions and information quality on the outcomes. Similar indications are also provided by Herath and Rao (2009b) who study security breaches in organizations. Their result show that both perceived severity (but not perceived probability) of security breaches, response efficacy and self-efficacy significantly impact the attitude towards compliance with security policy, and by Ifinedo (2012) who reports significance of both threat and coping appraisals. What is more, coping appraisal elements can also be impacted by the organizational involvement in promoting information security awareness, which is operationalized through the availability of resources and the employee commitment to the organization. Interestingly, Herath and Rao's study delivers contradicting results with regards to significance GDT elements – the perceived severity of punishment is negatively related to security policy compliance intentions.

The complex nature of information security awareness can also be found in Johnston and Warkentin (2010). Similar to other studies, coping appraisal has a significant effect on intention to comply with security policy, however, the elements of fear appeals (threats appraisal) are tested as antecedents of both self-efficacy and response efficacy. Interestingly enough, only perceived severity is significant in such configuration. Nevertheless, the above results throw additional light to the nature of information security awareness, and support the claim that it is a complex phenomenon that possibly consists of several dimensions – all of which need to be adequately addressed by an organization, if high levels of security awareness are to be achieved. It also appears that there is a lack of appropriate training on information security threats in organizational setting (Vance, Siponen, & Pahnila, 2012). As in personal settings, coping appraisal elements are significant predictors of intention to comply with security policies in most cases. However, it appears that risk analysis on individual level represented by different incarnations of perceived vulnerability is often not present in organizational security training efforts. More specifically, the levels of risk awareness differ between IS and non-IS professionals, and even between different industries (i.e., IT intensive industry vs. non-IT intensive industry (Y. Lee & Larsen, 2009). Furthermore, consistent compliant behaviors are more likely to occur if individuals feel threatened in comparison to situations where threats are perceived as not as imminent. Thus, organizations should carefully implement their visions of threats, since describing threat impact as unavoidable could potentially lead to fatalistic attitudes, and not improve compliance at all (Workman, Bommer, & Straub, 2008). The inconsistent results of individual studies indicate that different organizations may provide training (to their employees) that significantly differs in subject matter coverage. Another potential explanation of such discrepancies could be due to cultural differences (Warkentin, Malimage, & Malimage, 2012).

The extant area of information security research is grounded within other psychological theories, very often based on some variation of TRA, TPB, or TAM (Bulgurcu et al., 2010; Culnan, Foxman, & Ray, 2008; Dinev & Hu, 2007; Goodhue & Straub, 1989; Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011; Kumar, Mohan, & Holowczak, 2008; Pavlou, Huigang, & Yajiong, 2007), and sometimes combining elements from the aforementioned GDT and PMT.

Information Security Awareness

Summary of current research on information security awareness and information security training is presented in Table 1. Although the effects of training and education activities are not directly examined in the present study, it is important to include them. The present study is designed in such manner so that the results allow for quick identification of awareness deficiencies in individuals. The results of the previous studies on training are included to allow the reader to cross-validate the findings of the present study with the current body of knowledge, and provide a quick reference for more other readings on the topic. Up-to-date publications have been analyzed with regards to their approach to the definition of security awareness and recommendations towards training. The exact definition of security awareness is listed wherever a given publication provided one. Otherwise, the implied meaning is provided based on the context of a study.

Table 1

Summary of Current Research on Security Awareness and Security Training

Author	**Theoretical Foundations**	**Security Awareness**	**Training guidelines**
(Albrechtsen & Hovden, 2009)	N/A	Awareness of incidents, threats, vulnerabilities, and problems	
(Albrechtsen & Hovden, 2010)	N/A	Awareness consists of the following: responsibility, motivation, security vs. functionality, reporting, perceived skills and knowledge, importance of security means, importance of generic loss prevention means	Improve awareness through small-sized workshops that would emphasize employee participation, dialogue, and collective reflection

(table continues)

Table 1 *(continued)*

Author	Theoretical Foundations	Security Awareness	Training guidelines
(Albrechtsen, 2007)	N/A	The extent to which individuals understand the importance of information security; the level of security required by the organization and their individual security responsibilities.	Should influence the benefits of compliance, the expected costs of risky behaviors, and present cost of recommended behaviors as not time-consuming.
(Boss et al., 2009)	Organizational control theory, GDT	General awareness defined in terms of precaution taking that depends on specification of policies, evaluation of compliance with policies, and rewards for compliance. Also, mandatoriness is defined as a degree to which individuals perceive compliance with security policies compulsory or expected.	Should focus on improving computer self-efficacy
(Bulgurcu et al., 2010)	Rational choice theory, TPBr	Employee's general knowledge about information security and his cognizance of the information security policies (ISP) of his organization. General information security awareness and ISP awareness are the key dimensions of security awareness. General information security awareness is defined as an employee's overall knowledge and understanding of potential issues related to information security and their ramifications. ISP awareness is defined as an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements.	Training should help create security-aware culture that would increase information security awareness and self-efficacy about compliance
(Chen, Shaw, & Yang, 2006)	Based on NIST SP 800-16 (National Institute of Standards and Technology, 1998)	Following NIST SP 800-16. Security awareness efforts constitute active informing intended to change the behavior of users and reinforce good security practices.	Implemented through information security awareness system. Should be tied to individual needs. Should include: information portals, newsgroups, discussion forums, index of previous breaches, awareness activities, etc.
(Chan, Woon, & Kankanhalli, 2005)	Social information processing, safety climate	Conceptualized through self-efficacy of detecting security breaches.	SETA programs should actively implement policy guidelines and lessons learned
(Chang & Wang, 2011)		Not explicitly defined, implied awareness of CIA triad.	Training should outline roles and responsibilities that employees should follow to keep organizations secure.
(Cone, Irvine, Thompson, & Nguyen, 2007)	N/A	N/A	A video game approach, implementing CyberCEIGE.
(Crossler, 2010)	PMT	N/A, believed to be indirectly defined through coping and threat appraisals	Training should focus on self-efficacy and response efficacy.
(D'Arcy et al., 2009)	GDT	User awareness of security countermeasures (i.e., security policies, SETA programs, computer monitoring) impact severity and certainty of sanctions.	Transfer knowledge about information risks, emphasize recent reactions to policy violations, and raise awareness of responsibilities.

(table continues)

Table 1 *(continued)*

Author	**Theoretical Foundations**	**Security Awareness**	**Training guidelines**
(Dinev & Hu, 2007)	Technology acceptance model, TPB	Technology awareness – individual's raised consciousness of and interest in knowing about technological issues and strategies to deal with them.	Teaching users how to use protective technologies is not enough. Training should focus on the consequences of noncompliance.
(Dodge Jr, Carver, & Ferguson, 2007)	N/A	Discussed in the context of information assurance awareness, defined as a random variable that is difficult to characterize due to user's individual nature.	Training addressed through repeated exercises.
(Dowland, Furnell, Illingworth, & Reynolds, 1999)	N/A	Awareness of computer crime and abuse, and relevant legislation.	Raise awareness of corrective actions.
(Dutta & Roy, 2008)	Systems dynamics	N/A	Increase awareness and knowledge of technology, best practices and policies.
(Furnell, 2005)	N/A	Awareness of Internet threats.	Enable users to protect themselves, create knowledge in terms of finding, understanding, and using security technologies.
(Furnell, Bryant, & Phippen, 2007)	N/A	Awareness of threats and safeguards.	Focus on conveying a message that security is everybody's responsibility.
(Hagen, Albrechtsen, & Johnsen, 2011)	N/A	Knowledge of threats associated with CIA triad, traveling, personal security, physical security, communications security.	Training and education should be a continuous effort.
(Herath & Rao, 2009a)	Principal agent theory, GDT	Awareness of monitoring and detection performed by organizations.	Focus on intrinsic (perceived value and contribution) and extrinsic motivators (impact of penalties, social pressures)
(Herath & Rao, 2009b)	TPB, PMT, GDT	Not defined explicitly. Awareness could be conceptualized through coping and threat appraisals.	Focus on increasing self-efficacy, availability of facilitating conditions, availability of resource through posters, newsletters, notices, etc.
(Johnston & Warkentin, 2010)	PMT, fear appeal theory	Not directly stated. Implied as awareness of threats (perceived severity and susceptibility)	Address threat mitigation processes rather than performance gains. Focus on coping and threat appraisal processes.
(Karjalainen & Siponen, 2011)	N/A		Training approach that is composed of four stages: (1) involve concrete experiences, (2) engagement in reflective observation, (3) support formation of abstract concepts and generalizations, (4) enabling active experimentation.
(Kritzinger & Smith, 2008)	N/A	Information security awareness is about ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with	N/A

(table continues)

Table 1 *(continued)*

Author	**Theoretical Foundations**	**Security Awareness**	**Training guidelines**
(LaRose et al., 2008)	PMT, Social cognitive theory, Elaboration likelihood model	Not directly defined; however operationalized through threat appraisal.	Training promoted through focusing on motivational factors (protection motivation, rewards vs. costs, involvement, and self-regulation).
(Liang & Xue, 2009)	TTAT	Not explicitly defined. Awareness of existence of malicious information technology in the environment. Awareness is also created by comparing the potential effects of a threat with user's current state. Such comparison triggers proper coping behaviors. It is implied that awareness is focused on individuals' perceptions about threats and the availability of safeguarding measures, including the availability of information security policy.	Training should focus not only on the likelihood of being attacked by malicious information technology but also on negative outcomes that could affect users once they become victims.
(Liang & Xue, 2010)	TTAT	Not explicitly defined. However, implied through threat and coping appraisals.	SETA programs needed to help users cope with information technology threats.
(Ng, Kankanhalli, & Xu, 2009)	Health belief model	Awareness of threats and means of protection (perceived susceptibility, perceived benefits respectively).	Security awareness programs should educate users about the possibility and damage of security threats so they understand the need for security and their roles and responsibilities in protecting data and other information assets. Awareness messages should highlight severity and susceptibility. Awareness programs should train users on the purpose and functions of security controls, be it technical, physical, or human controls
(Pahnila et al., 2007)	GDT, PMT, TRA, information systems success model, Triandis' behavioral framework	Awareness of security policies and guidelines. Awareness of security threats and their severity and celerity. Implied relationship with coping and threat appraisals.	Not explicitly stated. Training should focus on motivational and attitudinal factors through the formation of proper coping and threat appraisals. It is also suggested that the quality of informational sessions is important
(Puhakainen & Siponen, 2010)	Universal constructive instructional theory, Elaboration likelihood model	N/A	Training should enable learners' systematic cognitive processing of information. Learning tasks should be relevant to learners. Training should account for users' previous experience. Training is believed to be a continuous effort that should emphasize motivational factors of recipients, ideally making them actively involved.

(table continues)

Table 1 *(continued)*

Author	**Theoretical Foundations**	**Security Awareness**	**Training guidelines**
(Rezgui & Marks, 2008)	N/A	Same as Siponen (Siponen, 2000).	Training should focus on informing users about information security threats and concerns and equip them with skills to support organizational security policies. Training should be regular and standardized. Supports implementation of reward and punishment system.
(Rhee, Kim, & Ryu, 2009)	Social cognitive theory	N/A	Training should focus on self-efficacy. Simply listing penalties for violations is not enough.
(Rhee, Ryu, & Kim, 2012)	Social cognitive theory	Awareness of information security is the vigilance in understanding various information security threats and in perceiving vulnerability related to these threats.	Should be systematic.
(Sasse, Brostoff, & Weirich, 2001)	N/A	Awareness of the consequences noncompliant behaviors, achieved through negative reinforcements.	Training should address the causes of undesirable behaviors.
(Shaw, Chen, Harris, & Huang, 2009)	Situation awareness (?)	Security awareness is the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks.	E-learning systems suggested as a feasible alternative to deliver SA programs (through information richness).
(Siponen & Vance, 2010)	Neutralization theory, GDT	N/A	Training should emphasize the negative consequences of noncompliant behaviors with regards to security policies. It should also focus on the fact that there is no excuse for failing to comply with those policies. It is also emphasized that sanctions are not effective deterrents.
(Siponen & Vance, 2013)	N/A	Awareness of information security policies and violations of those policies.	N/A
(Siponen, 2000)	TRA, TPB, intrinsic motivation, technology acceptance model	State where users in an organization are aware of - ideally committed to - their security mission (often expressed in end-user security guidelines). Increased awareness should minimize "user-related faults", nullify them in theory, and maximize the efficiency of security techniques and procedures. Two categories of awareness are proposed: framework and content.	Training should focus on underlying reasons responsible for human errors. Should be systematic and follow well-established frameworks (i.e., NIST). Author emphasizes the importance of attitudinal and motivational factors.
(Siponen, 2001)	N/A	Five dimensions of information security awareness: organizational, general public, socio-political, computer ethical, institutional education dimension. Those dimensions identify different stakeholders that contribute to the overall scope of information security awareness.	User education is one of dimensions of security awareness.

(table continues)

Table 1 *(continued)*

Author	**Theoretical Foundations**	**Security Awareness**	**Training guidelines**
(Siponen et al., 2006)	PMT, TRA	Security awareness not explicitly defined; however, awareness of security threats implied to influence cognitive processes of PMT	Training and education should be conducted in a visible manner. External visibility (news and commercials in media) of security is also important.
(Spears & Barki, 2010)	User participation theories	Organizational awareness of security risks and controls. It is associated with raised consciousness and en enhanced adoption of security policies and countermeasures.	This study advocates raising awareness by engaging users in the process of managing specific security risks within their business processes. By having users participate, security becomes more relevant to users and security measures become better aligned with business objectives.
(Straub & Welke, 1998)	GDT	Awareness of consequences of computer abuse and the impact of their countermeasures (both remedial and recovery).	Potent security awareness training stresses the two central tenets of general deterrence theory: certainty of sanctioning and severity of sanctioning. Structured approach is proposed. Also suggested use of reinforcing feedback that would consist an ongoing dissemination of security actions taken against violators and policies employed to prevent such violations.
(Straub, 1990)	GDT	Awareness of efforts to control anti-social behaviors.	Deterrence measures (i.e., policies, guidelines) and penalties are believed to be effective at improving security. Thus, training efforts should focus on disseminating information about consequences of exercising not recommended behaviors.
(Talib, Clarke, & Furnell, 2010)	N/A	Knowledge of threats.	Training knowledge transferred from workplace to home settings.
(Thomson & von Solms, 1998)	Social psychology theories	Not defined explicitly, implied awareness of security threats.	Educate users about information security issues, and continually remind of those issues, plus any new issues that become relevant. In addition to technical information, motivational factors affecting user behavior should also be included in the program. Social psychological principles need to be accounted for while designing the program.
(Tidwell, 2010)	N/A	Information security awareness can be described as the state where users are aware of, or attentive to, their security mission as expressed in end-user guidelines or the security policy (Siponen, 2000).	Training described as an ongoing effort.

(table continues)

Table 1 *(continued)*

Author	**Theoretical Foundations**	**Security Awareness**	**Training guidelines**
(Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008a)	N/A	The authors conduct a review of different perceptions of awareness. According to the results, it is not clear whether this term refers to a process, a product, or both. The study calls for more clarification on what information security awareness really is.	Awareness, education, and training perceived as three distinct components.
(Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008b)	N/A	Security awareness described as an organizational process characterized by: enhancing the adoption of security policies and countermeasures, improving individual behavior, altering work routines so that good security habits are applied.	N/A
(Vance et al., 2012)	PMT, habit theory	Awareness of threats believed to trigger the cognitive processes (i.e., threat and coping appraisals).	Companies must organize IS security seminars or training sessions where employees are made aware of possible IS security threats and their severity and speed. Training should focus on the consequences of lack of compliance with security policies.
(Vroom & von Solms, 2004)	Organizational culture model	Security awareness described as a state that depends on three levels of organizational behavior: individual, group, and formal organization.	Training should influence the cultural aspect of security, by addressing all three dimensions underlying information security awareness.
(Woon et al., 2005)	PMT	Awareness conceptualized as knowledge of a given topic.	Since the paper discusses home settings, training is conceptualized as provision of customized guidelines that would influence users' self-efficacy and response efficacy.
(Workman et al., 2008)	PMT, social cognitive theory	Awareness of pervasive security threats and countermeasures.	Focus on self-efficacy of dealing with security threats. Address underlying motivational factors.
(Y. Lee & Larsen, 2009)	PMT	Not explicitly defined; operationalized through threat and coping appraisals. Assumed that study participants are fully aware of malware threats and effectiveness of anti-malware software.	Continuous process, involving active presence of security vendors on-site.

The review of research publications on information security awareness reveals several very interesting insights on the phenomenon under investigation. First, there is a lack of consensus on what security awareness in fact is. Only several studies provide an explicit definition of the construct. While the concepts in each of them are similar, there is a lack of consistency in definitions. For example, some researchers define security awareness as understanding of the importance of information security along with the levels of security required by organizations, and consequently the related user responsibilities (Albrechtsen, 2007; Kritzinger & Smith, 2008). Others, refer to security awareness as to the level of knowledge about- and understanding of potential information security issues in organizations (Bulgurcu et al., 2010), awareness of threats (Ng et al., 2009; Pahnila et al., 2007; Rhee et al., 2012), awareness of security countermeasures and precautions (Boss et al., 2009; D'Arcy et al., 2009; Ng et al., 2009), and awareness of information security policies, guidelines, and other organizational instruments (e.g., computer monitoring, security training) (D'Arcy et al., 2009; Pahnila et al., 2007; Siponen & Vance, 2013; Siponen, 2000). Overall, those definitions are highly dependent on the context of study in which they are operationalized (e.g., compliance with security policies, protective behaviors, etc.). What is more, numerous other studies discuss the topic from a higher level of abstraction. That is, security awareness is discussed from a framework perspective; security awareness is presented as an overarching context within which underlying constructs are discussed. As result, the concept is not explicitly defined; however, variables that could potentially explain it are under investigation. More specifically, security awareness is often indirectly studied using theoretical frameworks like GDT or PMT. These approaches examine factors influencing recommended security behaviors of individuals. As discussed in the above paragraphs, these theoretical frameworks investigate external motivators (e.g., sanctions, rewards, etc.) or internal perceptions of information security issues (e.g., seriousness, severity of threats, vulnerability to risks, and perceived ability of handling such risks). Majority of the studies implementing PMT as the underlying theoretical lens emphasize the importance of formation of threat appraisal processes (i.e., estimating seriousness of a threat, and perceived risk of exposure), which are weighted against the formation of coping appraisals processes (i.e., self-beliefs of being able to exercise preventive behaviors, the degree of confidence to which such preventive behaviors will be effective with handling security threats, and perceived costs required to avoid security threats). Consequently, these studies share a common perception about information security threats, as well as similar approaches to be employed in order to handle the issues. More specifically, security threats have been investigated in terms of severity of their potential effects and consequences, and individual's or organization's susceptibility or vulnerability to being exposed to them. On the other hand, coping appraisals – usually operationalized through self-efficacy, response efficacy, and response costs – are the main constructs used to explain individuals' abilities to handle information security threats (Crossler, 2010; Johnston & Warkentin, 2010; LaRose et al., 2008; Y. Lee & Larsen, 2009; Liang & Xue, 2009; Siponen et al., 2006). Thus, despite the fact that those studies are not concerned with defining security awareness per se, they indirectly imply how security awareness should be approached and contextualized.

This lack of consistent definition of security awareness makes it difficult to compare results from different studies. As a result, there exists an evident need for universal conceptualization of information security awareness. Unfortunately, the literature does not provide direct evidence on what security awareness is. To address this gap, the first goal of the present study is to propose a concise yet comprehensive definition of information security awareness. Such definition could be used across various environments (i.e., home vs. workplace), and through different contextual applications. These applications could address topics like compliance with security policies, self-protection, examination of risky behaviors through enhancing the adoption of information security policies and countermeasures, improving individuals' security behaviors, or altering work routines in order to promote good security habits (Tsohou et al., 2008b).

Previous literature indicates that defining security awareness is not a straightforward process. The above review also indicates the possibility that the concept is in fact multidimensional which is also supported by Dodge Jr, et al. (2007), who suggest that awareness is a random variable, and because of user's individual nature it is very difficult to characterize. In addition, there seems to be a lack of certainty among researchers as to whether the actual term refers to process, a product, or both (Tsohou et al., 2008b). There is also lack of consensus on whether awareness encompasses training and education. Based on Merriam-Webster dictionary definition (2013), the present study makes an assumption that security awareness is a state of showing realization, perception, or knowledge, which needs to be continuously reevaluated. This approach is also compatible with widely accepted practitioner standards that explicitly distinguish between awareness and training. NIST SP 800-50 standard states that awareness is not training (National Institute of Standards and Technology, 2003). NIST SP 800-50 goes even a step further and provides a distinction between awareness activities and training. For the purpose of the present study, security awareness is separated from awareness activities in order to avoid confusion between process vs. state conceptualization. Previous attempts at unifying the view of awareness have clearly indicated that researchers often fall into the trap of ambiguity (Tsohou et al., 2008a, 2008b).

Information Security Awareness Definition

With regards to the definition of information security awareness, the present study attempts to answer the following research question:

Research Question 1 (RQ1): What is information security awareness and what are its dimensions?

In order to derive a complete definition of security awareness this study draws heavily on both academic and practitioner literature. The analysis of both streams of literature reveals that both researchers and practitioners in fact share similar mental model with regards to the concept of the phenomenon. However, the definition is still somewhat problematic. The review of academic research shows that security awareness is in fact a multidimensional construct, and that is why the IS field has not arrived at unified definition of the concept. At the same time, practitioner literature takes the meaning of security awareness for granted so to say. While practitioner publications often fail to define it, the prescriptive nature of non-academic literature often offers advice on how SETA programs should be designed in order to improve the overall security awareness of the programs' recipients (SANS Institute, 2013). A simple example will show the underlying assumptions of security awareness. As mentioned, according to NIST SP 800-50 and NIST SP 800-16 awareness is not training (National Institute of Standards and Technology, 1998, 2003). The standards also mention the purpose of awareness activities – to focus attention on security, and to allow individuals to recognize IT security concerns and respond accordingly. Such an approach is operationalized with an example of virus protection. The aftermath of such training session should result in individuals being able to describe what a virus is, what the potential consequences are in case a virus infects a system, what the users should do to protect the system, and what the users should do if a virus is discovered. Similarly, Rudolph et al. (2002) conclude that content of security awareness activities should include information about security risks (e.g., what does a threat look like) and vulnerabilities (e.g., how a threat might surface on local systems), basic countermeasures, user responsibilities, and incident reporting procedures.

Another important assumption that requires clarification is determining whether awareness is a state or a process. Both research and practitioner work in the field deliver inconclusive evidence about the nature of the construct itself. Therefore, a broader perspective needs to be introduced if security awareness is to be defined properly. Situation awareness is another concept that is important for defining security awareness in the present study. Having its roots in military training, situation awareness is defined as “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” (Endsley, 1995, p. 36). It is also important to note that situation awareness is a state of knowledge. Endsley also notes that it does not include the entirety of an individual’s knowledge. It only includes the fraction that refers to the current state of a dynamic environment (Endsley, Bolté, & Jones, 2003; Endsley, 1995). As such, it is applicable to the process of avoiding information security threats, where individuals are often required to make decisions based on the knowledge they can access in a limited period of time. That fraction of knowledge determines whether they are able to successfully avoid threats as they encounter them. Thus, awareness accounts for the temporal aspect of a given situation (i.e., exposure to a threat) (Sarter & Woods, 1991). As a result, situation awareness pertains to information that is available to individuals at a given point of time, or information that can quickly be activated (from previous representations of knowledge) when it is relevant to assess and cope with a given problem at hand (Kihlstrom & Cantor, 1984). From the perspective of the present study, the assessment of the situation and the devising a suitable coping response are the most important factors joining the concept of situation awareness with the prescriptions of PMT and TTAT. Since this study assumes that security awareness is a state, then it is a product of the learning activities, regardless of where such activities occur with regards to time and space (e.g., at workplace via training activities, or through personal experience). As result, individuals subjected to security awareness programs should show at least some degree of realization, perception, and knowledge about threats. Therefore, from a practical perspective:

Proposition 1 (P1): Security awareness should be defined as the state of knowing what a threat is and being able to define it, being able to recognize it, knowing the potential effects of a threat, having the knowledge and skills allowing threat avoidance, and knowing one's responsibilities with regards to threat avoidance and reporting discoveries of threats.

Such an approach reveals that security awareness is in fact composed of several distinct areas, which need to be orchestrated in synergy in order to consciously and effectively avoid security threats. A closer look at academic literature reveals that scholars, while often not being able to provide a complete conceptualization of security awareness, also share similar perspectives on the topic. Although often partially defined or not defined at all, the important elements of security awareness are present at least to some extent in every article included in Table 1. As discussed, when explicitly defined, the conceptualizations of security awareness are at least partially overlapping with the definition proposed in this study. When not explicitly stated, the discussions regarding security awareness often revolve around concepts related to threat appraisal and coping appraisal processes.

For theoretical conceptualization of information security awareness, the present research incorporates technology threat avoidance theory (TTAT) (Liang & Xue, 2009) as the underlying theoretical framework. TTAT has its roots in cybernetic theory and coping theory. TTAT provides a general framework through which individuals' security-related behaviors can be explained. The purpose of the framework is to explain the process and the determinants of threat avoidance behaviors across a broad range of IT threats and user populations. Compliance with information security policies is an example of such behaviors, since the expected outcome of compliance is the actual avoidance of threats. Although TTAT takes advantage of both process theories and variance theories, this study is focused on the latter approach as it is not concerned with the dynamic nature of security awareness (Markus & Robey, 1988). TTAT approach to security awareness is also well justified because it integrates various theoretical approaches, including PMT (Rogers, 1975, 1983), health belief model (HBM) (Rosenstock, 1974), and risk analysis (Baskerville, 1991). As result, the variance theory view of TTAT is composed of variables referring to threat appraisal, coping appraisal, and the actual coping. The below paragraphs draw the connection between the practitioner view of security awareness conceptualized in this study, and the theoretical view of awareness presented in TTAT.

As a result, it is shown that TTAT is the proper framework for describing phenomenon under investigation. However, TTAT model is designed for voluntary settings (Liang & Xue, 2010). This study is focused on mandatory settings in an organizational environment.

Therefore, the original TTAT model is extended and combined with GDT in order to reflect different nature of the problem.

TTAT posits that threat avoidance consists of threat appraisal processes, coping appraisal process, and actual coping behaviors. The above are nothing else than the assessment of situation and the projection of coping behaviors that should be implemented in order to cope with the situation. Which is exactly what the theoretical foundations of situation awareness prescribe (Endsley et al., 2003; Endsley & Garland, 2000; Endsley, 1995; Kihlstrom & Cantor, 1984). Consequently, there exists a valid theoretical linkage between situation awareness, and the assumptions of TTAT and PMT. The latter are described below.

Threat appraisal is composed of perceived susceptibility and perceived severity. The former refers to a person's perceived risk (i.e., probability) of being negatively affected by information security threats. On the other hand, the latter is associated with the degree to which a person believes that consequences of being affected by security threats are serious and severe. It is assumed that individuals will perceive something as a threat, if it is likely that they will be affected by it and when the consequences of such event are serious. These concepts capture the following element of the definitions of information security awareness posited in P1: knowledge of and ability to define threats, and understanding of potential consequences of them. More specifically, an individual can completely assess her levels of perceived severity and perceived susceptibility with regards to a given threat, if she knows what the threat is and what the potential consequences of such threat are. Consequently, accurate perceptions about the seriousness of a threat and the likelihood of being exposed to it can be estimated. The above assumptions are theoretically supported by the premises of PMT and HBM, which posit that threat appraisal processes motivate individuals to execute protective behaviors. While different individuals can demonstrate varied levels of threat appraisal for a given threat, it is the responsibility of SETA programs to educate them about the actual risks and magnitudes of various threats so that they can respond appropriately and accurately when a threat is discovered.

Whereas threat appraisal mechanisms are related to the understanding of the nature of threats, coping appraisal processes refer to perceptions about actions that could be employed as countermeasures of threats. TTAT assumes that coping behaviors include: perceived effectiveness of the safeguarding countermeasures, perceived costs related to such measures, and the degree of self-efficacy that individuals have about being able to exercise safeguarding behaviors (Liang & Xue, 2009). However, TTAT is designed for voluntary settings. In order to bring it to mandatory environments (i.e., compliance with organizational security policies), this study supplements TTAT view of coping appraisal with the degree to which individuals are aware of the responsibilities imposed on them by organizational policies with regards to threat avoidance behaviors.

Perceived self-efficacy can be defined as individuals' perceptions about the abilities to enact a designated level of performance that exercises influence over events impacting their lives. More importantly, individuals who demonstrate high levels of confidence in their own capabilities are more likely to perceive difficult problems as challenges rather than avoiding them (Bandura, 2010). In the context of this study though, avoidance of security threats is the expected behavior, often requiring certain levels of effort from the person enacting the avoidance behaviors. However, individuals with high levels of self-efficacy are able to take control over threatening situations as well. On the other hand, individuals with low levels of self-efficacy will tend to elude the threat avoidance behaviors, and express frustration caused by the potential obstacles (Compeau & Higgins, 1995). Self-efficacy is one of the major constructs forming protection motivation processes, and as such it has been examined in numerous academic publications on the topic (Crossler, 2010; Johnston & Warkentin, 2010; Siponen et al., 2006; Vance et al., 2012; Warkentin et al., 2012; Woon et al., 2005). From the perspective of the present research the formative processes of self-efficacy are extremely important. According to Bandura (2004), self-efficacy can be developed in four major ways: mastery experiences, social modeling (vicarious experiences), social persuasion, and construal of physical and emotional states. These indicators can be addressed by organizations through tools like training and awareness programs, or enforcement of information security policies. These formative processes best explain the underlying premises of the construct. That is, individuals can achieve high levels of self-efficacy with regards to security threats through experiencing them personally, by seeing other people handle such threats, or by being persuaded by the employer to comply. For example, previous research on information security has examined the effects of reward and punishment systems human attitudes and behaviors. In the context of information security, individuals may be required to cope with various kinds of threats ranging from purely technology-related like malware to human-oriented like social engineering.

Perceived effectiveness is the second dimension of coping appraisal mechanisms. It is defined as the degree to which individuals believe that the enactment of certain behaviors will lead to expected outcomes (Liang & Xue, 2009). Therefore, perceived effectiveness mirrors user beliefs with regards to outcomes of employing security threat countermeasures. The construct has its origins in outcome expectancy (Bandura, 1982, 2004). These behavioral outcomes can take three forms: material effects that the behavior produces, social approval or disapproval, and self-satisfaction. From the perspective of avoidance of security threats in organizational settings, it is expected that social approval may be of a larger importance in comparison to voluntary settings. In other words, satisfying the expectations of an employer may be an important factor influencing individuals' decisions about threat avoidance and compliance with information security policies. Perceived effectiveness is also, to some extent, similar to the concept of perceived benefits from HBM (Ng et al., 2009). In this case, the actual avoidance of a threat is considered to be beneficial either organization or for an individual herself. The issue however, is the fact that the benefits of threat avoidance behaviors may not be immediately visible to the individual. More importantly, the behavior, regardless of whether it is compliant with security expectations or not, and its consequences may be separated in time, and may not be directly observable by the individual. Other views of perceived effectiveness indicate its relatively close proximity to perceived usefulness from Technology Acceptance Model (TAM) (Davis, 1989), and performance expectancy as it has been updated in successive versions of TAM (Venkatesh, Morris, Davis, & Davis, 2003). Within TTAT, perceived effectiveness explains the usefulness of security safeguards with regards to their ability to help avoid security threats (Liang & Xue, 2009). As mentioned, these safeguards can come in different incarnations (e.g., compliance with security policy, usage of particular pieces of software, or exercising other types of behavior). As indicated by the literature however, there is a slight conceptual difference between perceived effectiveness and perceived usefulness. While the latter can be considered to be a construct measuring the overall effect in improvement of performance, the former applies to different context. According to Dinev and Hu (2007), information security should be treated as a protective technology, rather than a positive technology. With that assumption in mind, the two concepts, while sharing some similarities, are epistemologically different. Within the realm of information security, perceived effectiveness refers to avoidance of negative and harmful security threats rather than adoption of positive technologies. Nonetheless, it is also possible the avoidance of security threats could have an indirect impact on adoption of positive technologies that are aimed at improving individual's performance. For example, recent issues and concerns about Java zero-day security holes, can cause some enterprises to abandon the platform, because of the risks associated with the vulnerabilities discovered and migrate to rival solutions (Saran, 2013). The above situation is a perfect example of undoubtedly useful technology that may be discarded due to security concerns. In terms of perceived effectiveness, a researcher would be interested in the process of applying security updates provided by the vendor and their effectiveness in eliminating the vulnerabilities rather than improving the usefulness of the platform as a whole. The more detailed theoretical discussion on this interesting topic is outside of the scope of this study.

Finally, TTAT includes perceived costs of applying security safeguards to handle security threats as the last element of mechanisms regulating coping appraisals. They can be related not only to financial costs, but also to temporal and cognitive costs associated with avoidance behaviors (Liang & Xue, 2009). Practically, the costs associated with the enactment of threat avoidance behavior have negative impact on the latter. Individuals may feel overwhelmed with the burdens of specific countermeasures, and eventually abandon well-intended actions as high costs can create barriers to behavior. If for some reason the costs of threat avoidance outweigh the benefits than the likelihood of employing a security countermeasure is significantly lower. Prior research shows that costs of implementing security safeguards are negatively associated with individuals' attitudes towards such behaviors (Bulgurcu et al., 2010; Liang & Xue, 2010; Vance et al., 2012; Woon et al., 2005).

Now, TTAT framework is geared towards voluntary threat avoidance behaviors (Liang & Xue, 2010). Therefore, a factor accounting for the mandatoriness needs to be introduced to the concept in order to make TTAT applicable within organizational settings. While enterprises may be able to exercise some degree of control over their employees compliant behaviors (Warkentin & Johnston, 2008), at least some part of individual behaviors depends on their perception of the responsibility over protecting organizational information assets. Thus, on one hand organizations are expected to provide secure computing environment to their employees. On the other hand, due to the nature and the characteristics of some security threats, the employees are also responsible for maintaining desirable levels of information security in their organizations. Consequently, information security is everybody's responsibility. Organizations should clearly communicate this message, so that all employees are exactly aware what their duties are with regards to security threats and what is expected of them (Rudolph et al., 2002). In contrast, in voluntary settings, the sense of responsibility could be approached in terms of self-regulation – people are believed to act safely when their own personal standards of responsibility tell them to do so. Therefore, in voluntary settings responsibility is more closely related to moral attitudes, while in organizational settings responsibility is associated with knowledge and understanding of the behaviors expected by the employer in the event of discovery of security threats. As a result, responsibility can have an utterly different meaning depending on the context in which it is applied. Thus, within organizational settings, individual's responsibility for security is part of security awareness state as it is reflecting the fulfillment of employer's expectations towards the employees. At the same time, it is expected that the latter will be aware of such expectations, and thus know their responsibilities.

The above discussion draws parallels between practitioner approach to information security awareness (as described in P1), and current theoretical developments within academic research. The analysis indicates that both fields are not far apart in their understanding of information security awareness. Moreover, despite the fact that both fields often struggle with providing a comprehensive approach to the meaning of awareness, they are also very close in the way in which they approach awareness. Yet, neither practitioners nor scholars have been able to reach a consensus on what the term truly means. The above integrative analysis also indicates that the proposed definition of information security awareness in organizations can be explained through existing theoretical framework – Technology Threat Avoidance Theory. TTAT's constructs capture the essence of the state of security awareness. Therefore:

Proposition 2 (P2): Technology threat avoidance theory threat appraisal and coping appraisal processes extended with perceived knowledge of individual responsibilities capture the essence of the definition of security awareness (P1), and as such can be used to explain the levels of information security awareness in individuals.

Research Question 2 (RQ2): What are the antecedents of information security awareness?

Research Model

Although TTAT does not identify the antecedents of coping and threat appraisals, these are properly defined by PMT. Following the latter the antecedents of security awareness can all be captured under sources of information category. Sources of information can be divided into environmental sources (e.g., communication, observational learning) and intrapersonal sources (e.g., personality variables, prior experience) (Milne, Sheeran, & Orbell, 2000). The former can be represented by individual's awareness of the organizational information security policy (ISPA) and interest in information security issues (IIS). Information security policy is nothing else but a formal form of communication through which members of an organization can learn about the protections that the organization implements and enforces in order to protect its assets (Ciampa, 2010). In most cases security policy consists of more than one document. Separate documents can address issues like email policies, hiring and termination, personal information, acceptable use policy, or even policies for implementing specific countermeasures and resources (Boyle & Panko, 2013). Regardless of their focus, all policies have one thing in common – they outline what an organization's expectations are towards the employees. Thus, the employees can learn about their responsibilities with regards how to handle and avoid threats.

Aside from what is formally expected from the employees, they can also acquire knowledge about security threats through the exploration of their own personal interests in information security (i.e., through observational learning). In this case, it is assumed that a person plans to learn about security threats so that she can avoid them in the future; or that she is interested in learning as much as possible about the topic before forming an opinion.

Moreover, such highly motivated individuals may be interested in acquiring more knowledge about security threats so that they can apply it outside of the workplace, in their personal lives as well. Thus, the environmental sources of information are captured through two major constructs: information security policy awareness (ISPA) and personal interest in information security (IIS). ISPA is defined as the employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements (Bulgurcu et al., 2010). IIS is defined as motivation to receive judgment-relevant information that is as close to reality as possible (Darke et al., 1998; Todorov, Chaiken, & Henderson, 2002), as well as raised consciousness of and interest in knowing about security threats and strategies to deal with them (Dinev & Hu, 2007). These two constructs capture the external sources of information from which humans can build their security awareness (SA). At the other end of the spectrum, people can also acquire information from internal sources. Personality variables are not the essential part of the present study, and as such they are not included in the research model. However, prior experience (PE) is an important factor that can affect individual's security awareness. It is defined as previous conscious exposure to a threat. It is possible that person has been exposed to a security threat before, but she has failed to realize it. In such situations, she would have no prior experience. In this study, prior experience refers to situations where the individual knew about the presence of a threat (regardless of whether she suffered from the negative consequences of the threat). For example, if a person has previous experience with a computer virus, it is likely that she may already know whether she was exposed to severe consequences from the infection as well as the likelihood of being affected by a virus again. She may also know to recognize a virus in the future, and how to effectively avoid it. Thus, prior experience can influence both threat and coping appraisals. In addition, in organizational settings, and individual may already know what her responsibilities are with regards to threat avoidance. On the other hand, an employee that has not encountered a virus before may not necessarily know how the threat should be handled. Therefore, it is hypothesized:

H1: Individuals’ previous experience with information security threats will positively affect information security awareness.

H2: Individuals’ interest to learn about information security threats will positively affect information security awareness.

H3: Individuals’ information security policy awareness will positively affect information security awareness.

Information security policies can actually serve a dual purpose. Apart from educating the users about threats, they also carry another important bit of information. More specifically, they often inform the members of an organization about both positive and negative consequences resulting from compliance or lack of thereof. These consequences, for example, can include promotions and demotions, financial rewards and penalties, or other types of rewards and sanctions. These are in essence captured by two constructs sanctions (SAN) and rewards (REW). Sanctions are defined as tangible or intangible penalties - such as demotions, loss of reputation, reprimands, monetary or nonmonetary penalties, and unfavorable personal mention in oral or written assessment reports—incurred by an employee for noncompliance. Rewards are defined as tangible or intangible compensation that an organization gives to an employee in return for compliance (Bulgurcu et al., 2010). These two constructs represent the elements of basic deterrence approaches, which should be clearly communicated to the employees, usually through a basic information security training conducted upon hiring of a person. Consequently, if the human resources department exercises due diligence in its hiring practices, every new hire should know the general prescriptions included in the information security policy. Knowledge about sanctions and rewards (for noncompliance and compliance respectively) is not part of security awareness, as it does not inform the individuals about how to handle security threats. Thus, it is hypothesized that:

H4: Information security policy awareness will positively affect knowledge about rewards for compliance.

H5: Information security policy awareness will positively affect knowledge about sanctions for non-compliance.

Per the prescription of TPB and TRA, behavioral intentions of the individuals are derived from the attitudes. These, in turn can be affected in two ways. First, individuals who have security awareness about information security threats will be able to evaluate a threat in terms of its risk factors (i.e., severity and susceptibility), as well as respective threat avoidance factors (i.e., self-efficacy, effectiveness of avoidance, responsibilities, and cost of avoidance). Consequently, employees with high levels of security awareness (SA) should develop a more positive attitude towards compliance information security policies (ATT). Attitude is defined as the degree to which the performance of the compliance behavior is positively valued (Ajzen, 1991, 2005). It is so, because such individuals will be able to perceive compliance as a necessary and important step required for the effective protection of the organizational information assets. They will also be able to conceptualize and foresee the benefits resulting from compliance and its general usefulness. Such individuals will no longer perceive information security as a burden. On the contrary, they should understand how information security fits within the holistic perspective of their organization. It is also possible that, in general positive attitude towards compliance may lead to increased levels of security awareness. It is however beyond the scope of the present study. Second, attitudes towards compliance can also be affected by the knowledge about sanctions and rewards enforced by the parent organization. That is, if a person knows she may be rewarded for staying in compliance with the security policy, she may also develop a more positive attitude towards compliance due to the foreseeable benefits resulting from the process. On the other hand, a person may also develop a more positive attitude towards compliance if she fears the sanctions that can be incurred from noncompliant behaviors. Thus, the attitudes towards compliance with security policies can be affected by both the knowledge of an individual and by motivational factors enforced by the employer. Thus, it is hypothesized that:

H6: Information security awareness will positively affect individual's attitude towards compliance with information security policy.

H7: Rewards will positively affect individual's attitude towards compliance with information security policy.

H8: Sanctions will positively affect individual's attitude towards compliance with information security policy.

Following TPB (Ajzen, 2005; Madden, Ellen, & Ajzen, 1992), individuals' attitude towards security is defined as the degree to which they positively value the need to learn about information security threats in organizational settings which is exemplified through compliance with organizational security requirements. Consequently, if an individual perceives that achieving high levels of security awareness is beneficial to her, then she is more likely to develop a positive attitude towards information security. On the other hand, if she believes that the benefits of learning about security are low, then her attitude will tend to be more negative. Depending on the attitude, individuals may decide whether to comply with organizational requirements for information security. Therefore, it is hypothesized that:

H9: Attitude will positively affect intention to comply with information security policy.

H10: Security awareness will positively affect intention to comply with information security policy.

The final research model for this study is presented in Figure 1.

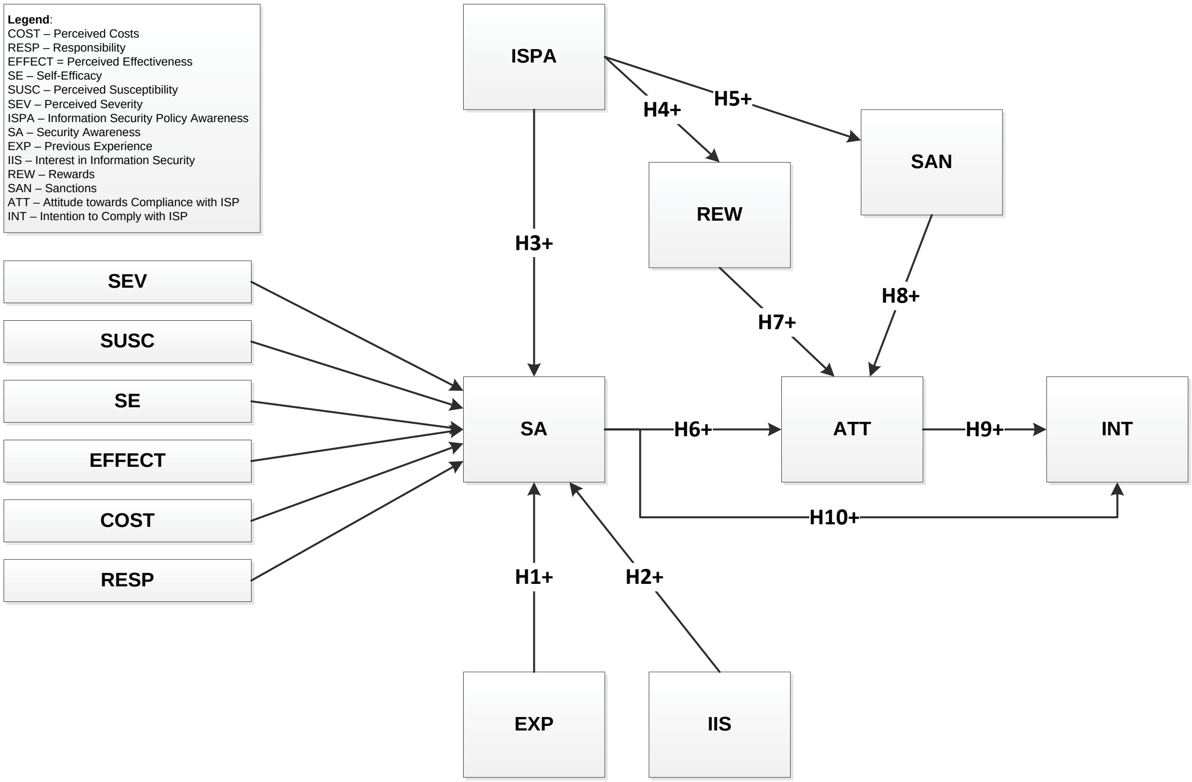

Legend:
COST – Perceived Costs
RESP – Responsibility
EFFECT = Perceived Effectiveness
SE – Self-Efficacy
SUSC – Perceived Susceptibility
SEV – Perceived Severity
ISPA – Information Security Policy Awareness
SA – Security Awareness
EXP – Previous Experience
IIS – Interest in Information Security
REW – Rewards
SAN – Sanctions
ATT – Attitude towards Compliance with ISP
INT – Intention to Comply with ISP
ISPA
H4+
H5+
SAN
REW
H3+
H8+
H7+
SEV
SUSC
SE
EFFECT
COST
RESP
SA
H6+
ATT
H9+
INT
H10+
H1+
H2+
EXP
IIS

Figure 1. Research model of security awareness and its antecedents.

CHAPTER 3

METHODOLOGY

This chapter outlines the methodology implemented to test the research model and its hypotheses presented in Figure 1. Following paragraphs describe the development process of the instrument and data collection procedures. The chapter discusses the following information: (1) population and sample, (2) unit of analysis, (3) instrument design and development, (4) instrument administration, and (5) data analysis strategy.

Population and Sample

The study has been conducted in cooperation with a municipal organization in the southwestern part of the United States. The main goal of the study is to evaluate information security awareness among individuals and to examine the impact of security awareness on compliance with organizational information security policy. The municipality under investigation employs over fourteen hundred full-time and part-time employees across numerous departments, including the services that are essential for the local community to function. The municipality has been chosen because its employees encounter information security threats in their everyday work routines. Furthermore, the municipality's information technology (IT) management group implements continuous monitoring of organization's IT infrastructure and services, reporting numerous cybercriminal attempts aimed at defeating organization's security defenses. Therefore, the management of the municipality is interested in maintaining its information security at a highest possible standard. The management also realizes that humans are the weakest link in security and wants to make sure that the employees are well-prepared to face information security threats. The municipality has an information security policy in place; however it wants to evaluate its employees in terms of potential deficiencies and areas for improvement in terms of their information security awareness. The results of the study are expected to serve as a foundation for a new information security training initiative, as well as future continuous reinforcements so that the municipality’s employees are able to handle a vast range of information security threats, and thus, protect organizational assets, and contribute to the well-functioning of the local community (i.e., maintain compliance with organizational information security policy).

Unit of Analysis

Since this study investigates information security awareness among the employees of an organization, the unit of analysis appropriate for this type of study is set at the individual level. This study has been designed investigate individual levels of information security awareness, and to account for its effects on compliance with the information security policy. Furthermore, individual has been chosen as the unit of analysis because the organization needs to account for different characteristics of its employees, and deliver information security training that would address the needs of all the employees, since all of them can be exposed to security threats resulting in a compromise of organizational information assets.

Instrument Design and Development

This study has been designed to be executed in two stages. In the first stage, the employees of the municipality have been exposed to a phishing experiment in order to directly observe their behavior with regards to compliance with the organization’s information security policy. A phishing experiment has been designed in order to lure the customer’s employees into clicking on a fake hyperlink sent within an email message. Phishing experiment has been chosen from other alternative behavior observation methods, because the IT management of the municipality has observed increased malicious activity in that area, and was interested in establishing whether some of the employees were more vulnerable to phishing attacks than others. It was also fairly easy to implement. The customer's employees have not been notified that the experiment took place.

In the second stage, following the phishing experiment, a survey instrument has been administered to the employees in order to collect information about their information security awareness levels and to examine the hypotheses from the research model. Also, the direct observation of behavior in the phishing experiment has been intentionally separated from the self-reported questionnaire instrument to account for potential common method bias issues (Podsakoff, MacKenzie, Jeong-Yeon, & Podsakoff, 2003). Both stages of the study have been designed and executed in close collaboration with the municipality's officials, so that the outcome of this study could serve as foundation for future implementations of information security awareness and training programs within the organization. The following paragraphs describe in detail the design process of both stages of the investigation.

The design process of the phishing experiment has been conducted with two primary objectives in mind. First, the municipality's IT management was interested in describing the characteristics of the individuals vulnerable to phishing attempts. The second objective was to examine different types of phishing with regards to their effects on the employees' phishability.

Phishing can be described as "the act of obtaining personal information directly from the user through the Internet" (Lininger & Vines, 2005, p. 8) or as "a type of social engineering, a high-tech scam that uses e-mail or websites to deceive people into disclosing personal information useful in identity theft, such as credit card numbers, bank account information, SSN, passwords, or other sensitive information" (Department of Defense). In a more general statement, it is the act of sending a forged email (in most instances using a bulk mailer) to an individual or a group of individuals, in which a phisher (i.e., a criminal who sets up a phishing scam) attempts to lure her victim into disclosing private information , such as credit card numbers, passwords, etc. In most cases, the fake email closely imitates a legitimate entity in order to gain the recipient's trust (James, 2009).

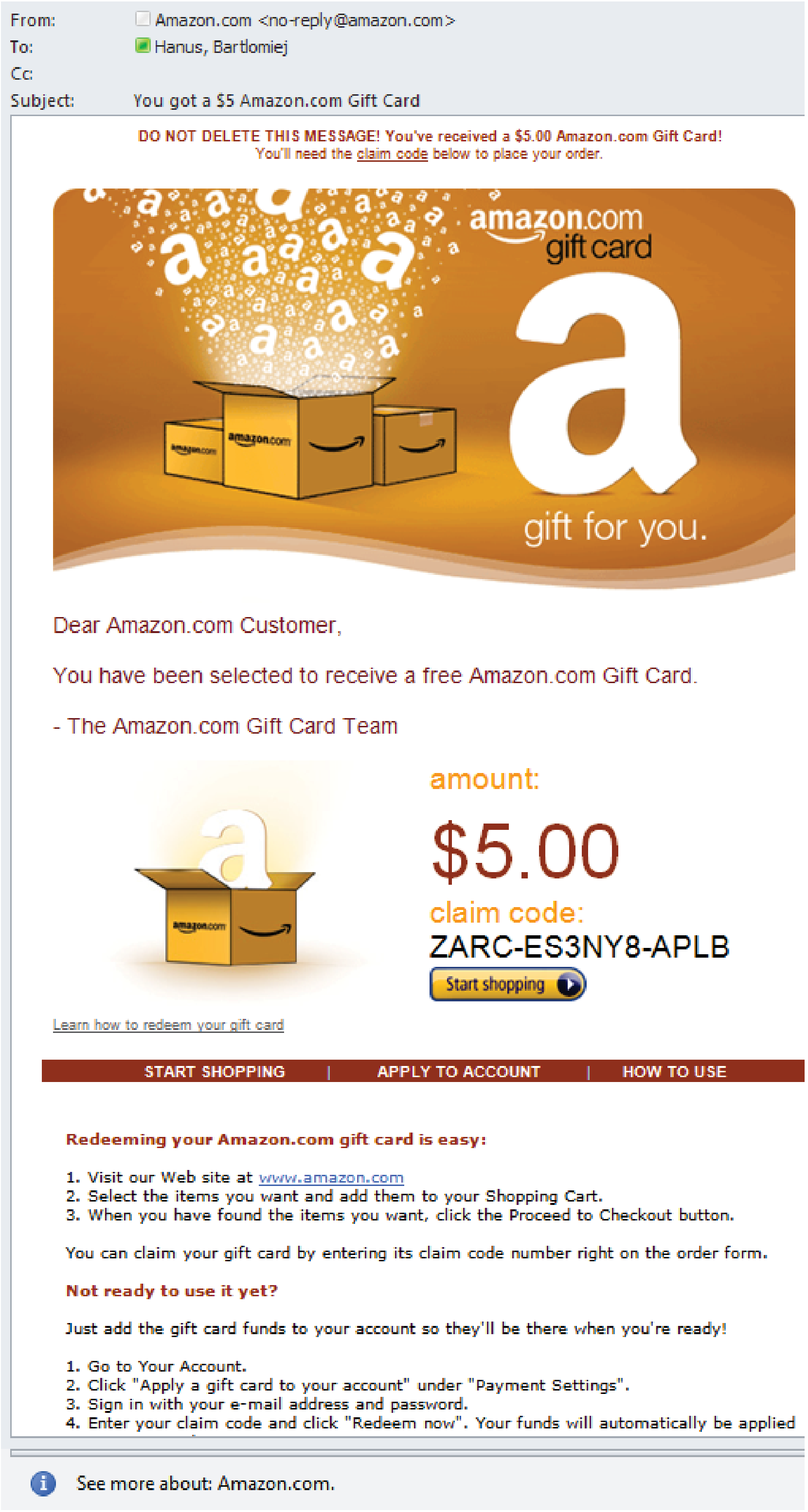
In a broader perspective, phishing falls under the umbrella of spam. The major categories of spam include unsolicited commercial email (UCE), nonresponsive commercial email (NCE), list makers, and scams. UCE messages are created by legitimate companies that attempt to advertise themselves to either existing or prospective customers. This category of spam accounts for approximately 0.1% of all spam messages worldwide. On the other hand, NCEs represent a more invasive instantiation of UCEs. They are also being sent by legitimate organizations, with the main difference being the fact that the customer has already opted out from the email list, but she still receives the unwanted correspondence. List makers are nothing else than spam groups harvesting email addresses with the purpose of selling them to other entities (both legitimate marketing organizations as well as other spammers). The last category of spam – scams, accounts for the majority of spam, and their main goal is to acquire assets through misrepresentation. Scams include for example, 419 scams, malware, and phishing.

Kaspersky Labs (2013) estimates that while spam in general accounts for approximately 70% of the total email traffic worldwide, phishing emails account for less than 1% of that traffic. Currently phishing attempts primarily target social networking sites (34% of all phishing), but financial, e-pay organizations, and banks remain the second largest phishing target (estimated at approximately 15%). Online stores and e-auctions account for 7% of all phishing. Phishing attempts on government organizations have relatively small share in total number of phishing attempts (i.e., less than 1%). While the total number of phishing attempts may seem relatively small in comparison to all spam activity, it has to be remembered that phishing malicious activities imitate existing entities, ergo its small share in total spam. However, in the absolute numbers perspective, phishing activity remains an important concern for information security professionals. For example, there were over 70,000 unique phishing attacks worldwide in 2013 (APWG, 2013). In addition, phishing sites are not online for an extended period of time. Once the phishing scheme is executed, usually the first 24 hours is when the phishers expect most of the traffic (APWG, 2013; James, 2009). Furthermore, the above statistics refer to a large extent only to regular phishing (note that different categories of phishing are discussed in the following paragraphs). Most of the spear-phishing attacks are usually not reported and it is generally not known how many of the spear-phishing attacks actually take place (APWG, 2013).

From a conceptual point of view, phishing can be divided into three major categories: regular phishing, spear-phishing, and whale phishing (also known as whaling). Regular phishing attacks do not target any specific group of individuals and are usually contextualized as an email message sent to a large group of people that generally do not have anything in common. The goal of the attacker is to reach as many individuals as possible, hoping that at least a small fraction of them falls victim to the attack. In such cases, even a very small response rate could result in significant gains for the cybercriminal. Regular phishing is widely used mostly because of its low cost of implementation. It costs as low as $10 to send 1 million emails, plus as low as

$5 to establish a fake web site or as low as $50 for a prepaid phishing domain (Goncharov, 2012). Spear-phishing attacks target a smaller, more select group of individuals (e.g. users of a specific website, members of an organization, employees of a company, etc.) with the primary goal of bypassing the security perimeter of the target organization. Spear-phishing is different from regular phishing in several ways. First, it often uses relevant contextual information to trick the target audience into disclosing personal information (Hong, 2012). Second, it often appears as if the email message has been sent from another member of the organization, preferably someone in a position of authority, so that the victim feels more pressured to comply with the message's request (Information Assurance Support Environment, 2013). In such circumstances, people who normally would not fall victim to phishing are up to four and a half times more likely to comply with the phisher's request due to the context (Hong, 2012). The last category of phishing is known as whaling. It is a special case of spear-phishing targeting senior executives or other high-level officials in an organization. In whale-phishing, attackers attempt to personalize the content of the message for a given individual by collecting information from the victim's online profiles, organization's website, etc. Another key distinction is that whaling emails hardly ever attempt to obtain financial information (Information Assurance Support Environment, 2013). Both spear-phishing and whaling could be significant tools in executing advanced persistent threats (APT) and targeted attacks.

For the purpose of this study, two types of phishing attacks have been designed. First – a regular phishing email message mimicking a free coupon from an online retailer. Second – a spear-phishing message targeting specifically the employees of the municipality. The content of both messages is presented in Figures 2 and 3. The design process of the spear-phishing email has been preceded by an in-depth analysis of the information available on the municipality's website. Based on the gathered information, the author has determined the organizational structure of the customer's IT department, including the software platforms employed by the organization. Next, the proposed content of both phishing emails has been presented to the municipality's IT management for approval. Both types of the phishing emails have been sent over the period of four weeks in January 2013. First, the employees have been exposed to the regular phishing email, and after four weeks the spear-phishing email has been sent. All of the hyperlinks in both email messages were pointing to a website on the authors's web server. Also, the sender's email addresses have been changed to reflect either an address belonging to the online retailer's domain, or to one of the IT helpdesk managers at the municipality. Prior to sending both phishing messages, a MD5 hash has been calculated for each individual's email address for the purpose of matching behaviors observed in the phishing experiment with the employee's responses to the survey instrument. All of the hyperlinks in the body of both messages have been customized to include the MD5 hash in the URL.



From: Amazon.com <no-reply@amazon.com>

To: Hanus, Bartlomiej

Cc:

Subject: You got a $5 Amazon.com Gift Card

DO NOT DELETE THIS MESSAGE! You've received a $5.00 Amazon.com Gift Card!
You'll need the claim code below to place your order.

amazon.com
gift card
gift for you.
amazon.com

Dear Amazon.com Customer,

You have been selected to receive a free Amazon.com Gift Card.

- The Amazon.com Gift Card Team

amount:

$5.00

claim code:

ZARC-ES3NY8-APLB

Start shopping
Learn how to redeem your gift card
START SHOPPING | APPLY TO ACCOUNT | HOW TO USE

Redeeming your Amazon.com gift card is easy:

1. Visit our Web site at www.amazon.com
2. Select the items you want and add them to your Shopping Cart.
3. When you have found the items you want, click the Proceed to Checkout button.

You can claim your gift card by entering its claim code number right on the order form.

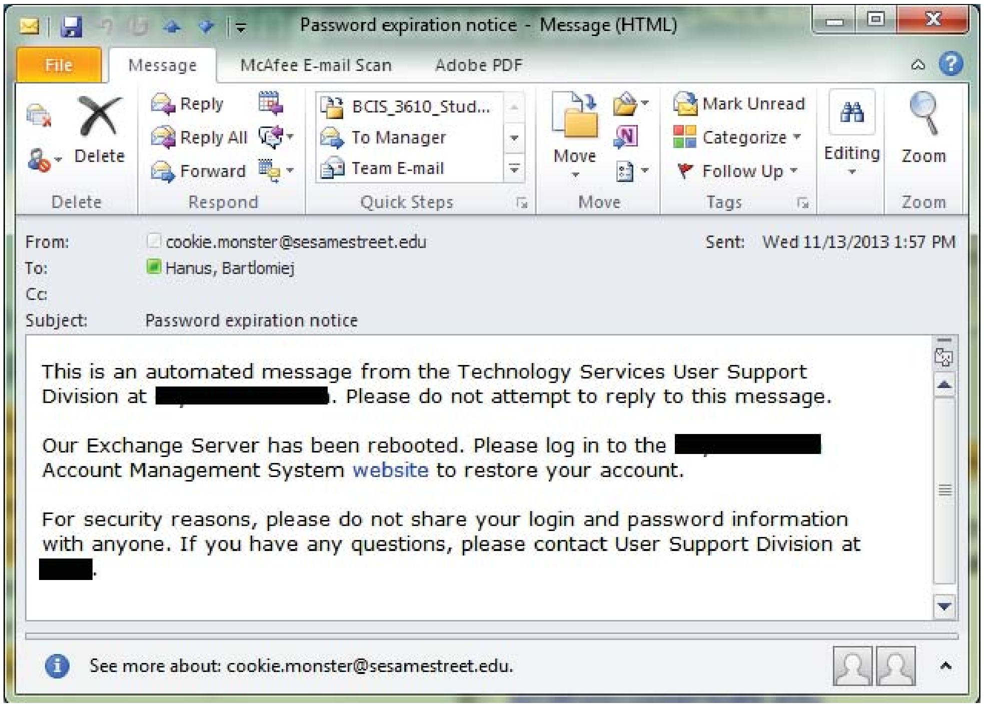
Not ready to use it yet?

Just add the gift card funds to your account so they'll be there when you're ready!

1. Go to Your Account.
2. Click "Apply a gift card to your account" under "Payment Settings".
3. Sign in with your e-mail address and password.
4. Enter your claim code and click "Redeem now". Your funds will automatically be applied

See more about: Amazon.com.

Figure 2. Regular phishing email.



From: cookie.monster@sesamestreet.edu
Sent: Wed 11/13/2013 1:57 PM
To: Hanus, Bartlomiej
Cc:
Subject: Password expiration notice

This is an automated message from the Technology Services User Support Division at [redacted]. Please do not attempt to reply to this message.

Our Exchange Server has been rebooted. Please log in to the [redacted] Account Management System website to restore your account.

For security reasons, please do not share your login and password information with anyone. If you have any questions, please contact User Support Division at [redacted].

See more about: cookie.monster@sesamestreet.edu.

Figure 3. Spear-phishing attack.

Once the municipality's employees received the forged messages, and decided to click on one of the hyperlinks, they were redirected to the author's website where each individual's MD5 hash identifier was extracted and stored in a database along with the type of phishing email she had clicked on. No other information that would allow for personal identification of any individual was collected. Once the MD5 hash information was written to the database, the victims were redirected to a legitimate website (i.e., either the online retailer's page or the municipality's home page). As a result, unless a given individual has examined any of the hyperlinks in the body of the message, they were not aware they have visited the author's web page prior to being redirected to the legitimate website.

A survey instrument was developed to conduct the second stage of the study and to test the research hypotheses. Survey approach has been chosen for several reasons. First, it allows for the measurement of a wide range of unobservable data, including individuals' traits (e.g. self-efficacy), attitudes (towards information security), or beliefs. Second, surveys are excellent tools for collecting data remotely, especially when the target population is too large to be observed directly. In case of this study, the employees of the municipality were not located within one site. Therefore, it was much easier to reach to them through an online survey. Third, surveys instruments provide a fair amount of flexibility for the participants as they can as respond to the questionnaire at their own convenience (Bhattacherjee, 2012; Kerlinger & Lee, 2000). On the other hand, surveys research has several disadvantages, including non-response bias, sampling bias, social desirability bias, or same source bias from self-reports (i.e., common method variance) (Bhattacherjee, 2012; Kerlinger & Lee, 2000; Podsakoff et al., 2003). During the design of the survey instrument the author has attempted to minimize the negative effects of the above issues by making sure that: the questions were not worded in a negative manner, the questions were clear and understandable and not ambiguous, and the questions contained just the right amount of detail. By making the survey anonymous, the issue of socially desirable answer bias has been addressed at least to some extent. Finally, because the study has separated direct observation of the behavior (vide the phishing experiment) from the survey instrument, the problem of common method variance has also been accounted for.

The item development process was initiated by a thorough and comprehensive review of the current literature. After identifying the constructs, the measurement items have been developed based on existing scales whenever possible. All of the constructs, with the exception of the expected second order construct for security awareness, have been measured reflectively on a seven-point Likert scale. The summary of the measurement items is presented in Table 2. A detailed listing of all of the questionnaire items is included in Appendix A.

Table 2

Summary of Measurement Items

Construct	Type	Source	Items
Security Awareness (SA)	Formative	latent variable scores for SEV, SUSC, SE, EFFECT, COST, RESP	6
Perceived Severity (SEV)	Reflective	(Ng et al., 2009; Witte, Cameron, McKeon, & Berkowitz, 1996)	4
Perceived Susceptibility (SUSC)	Reflective	(Liang & Xue, 2010; Rosenstock, 1974; Weinstein, 2000)	4
Self-Efficacy (SE)	Reflective	(Compeau & Higgins, 1995)	4
Perceived Effectiveness (EFFECT)	Reflective	(Ellen, Wiener, & Cobb-Walgren, 1991; Feinberg, Greenberg, & Osgood, 2004; Fishbein, Hall-Jamieson, Zimmer, von Haeften, & Nabi, 2002)	3
Perceived Costs (COST)	Reflective	(Vance et al., 2012; Woon et al., 2005)	2
Perceived Responsibility (RESP)	Reflective	self-developed based on Albrechtsen and Hovden (2010)	3
Information Security Policy Awareness (ISPA)	Reflective	(Bulgurcu et al., 2010)	4
Rewards (REW)	Reflective	(Bulgurcu et al., 2010; Kirsch & Boss, 2007)	3
Sanctions (SAN)	Reflective	(Bulgurcu et al., 2010; Kirsch & Boss, 2007)	3
Previous Experience w/ Threats (EXP)	Reflective	self-developed based on Darke et al. (1998)	3
Interest in Information Security (IIS)	Reflective	self-developed based on Dinev and Hu (2007) and Taylor, Wayment, and Carrillo (1996)	5
Attitude (ATT)	Reflective	(Ajzen, 1991)	4
Intention to Comply (INT)	Reflective	(Ajzen, 1991)	3

During the item development process, the initial design of the instrument was subjected to face validity verification performed at two levels. First, the instrument was presented to a group of experienced researchers and the feedback received was used to modify the instrument design. Second, the modified instrument was presented to the IT management of the customer. At both levels changes were made with regards to the wording of the measurement items, the scope of the instrument as a whole, and the overall instrument length. Per request of the customer, the initial questionnaire was shortened to account for potential respondent fatigue issue. As a result, different types of information security threats have been collapsed into three major categories of threats: personal, organizational, and technical. This categorization has been established based on the vulnerabilities that are specifically related to one these three areas. The categorization schema has been in detail discussed with both the three expert IS researchers and members of the municipality's IT management team, as well as based on the industry standards (ISO/IEC, 2005). In the introduction to the survey instrument, the purpose of the study was explained to the participants, along with the definition of an information security threat, as well as the three above dimensions of security threats. For further details, please refer to Appendix A. The final design represents a trade-off between the survey length and the expected level of depth. It should be mentioned at this point that personal threats were the primary area of interest in this study. However, the author also collected data on the remaining two dimensions with the aim of testing for the differences between the three categories of threats.

As a next step, the author developed an online questionnaire which was subject to approval of both – the three expert researchers and the municipality's IT management representatives. Once approved, the survey instrument was implemented in a pilot test. A convenience sample of undergraduate students enrolled in an introductory management information systems course was selected to voluntarily participate in the questionnaire. The questionnaire was designed with the focus on individuals who are employed by the customer organization. In a pilot study, all of the information related to the municipality was removed. The pilot study participants had already been introduced to basic concepts of information security in one of their prior lectures. Because undergraduate students might not necessarily be a representative sample of the municipality's employee population, before participating in the questionnaire, these individuals had been introduced to a scenario in which they were hypothesized to be members of a fictional organization. They were also introduced to a sample information security policy, and then asked to participate in the survey at their own convenience. The pilot study resulted in 74 usable responses, which have been subsequently assessed for reliability and validity tests, all of which exceeded acceptable thresholds for Cronbach’s alpha and factor loadings in exploratory factor analysis (Hair, Black, Babin, & Anderson, 2010). Based on the above steps, the instrument was determined to be adequate for the context of the study and ready to be used in the main study.

Instrument Administration

The main survey link was sent out be the municipality’s IT department. The email message contained a short description of why participation was important to the organization and it also informed the employees that the results would be anonymous. Approximately within one week intervals, a follow-up message was sent by the municipality’s IT manager encouraging those who had not participated in the survey yet to do so. The survey link was customized for each individual by adding a MD5 hash to the URL. Once an individual connected to the survey web site, the hash was extracted from the hyperlink and stored along with the individual’s responses. This way the researcher was able to match the survey respondents with the victims of the phishing experiment. Participation in the survey was voluntary.

Data Analysis Strategy

Data analysis in this research was conducted in two stages. First, discriminant analysis approach was used to analyze the characteristics of the victims of the phishing experiment. The author has obtained demographic information of all the individuals employed by the municipality. This information did not contain individual names. Instead, it contained MD5 hash replacing each person's email address.

Discriminant analysis is an appropriate data analysis technique in situations where the single dependent variable is dichotomous. In case of this research, an individual could either click on the phishing email link or ignore it (or even report it). Either of the behaviors is an instantiation of compliance with information security policy or lack of thereof. Discriminant analysis tests the hypothesis that the group means of a set of independent variables for two groups are equal. Moreover, the mechanics behind discriminant analysis are very similar to regression analysis. Like in the latter, it is a linear function of some number of independent variables used to predict a single dependent variable. However, unlike regression, discriminant analysis is applicable to cases where the dependent variable is categorical (i.e., nominal or nonmetric) (Hair et al., 2010). Therefore, this study employs discriminant analysis to investigate whether employee demographic characteristics can be used to predict their susceptibility to phishing. If so, it will also allow determining which characteristics account for most differences in the mean scores between the two groups (i.e., the individuals who "got phished" and those who did not).

Testing the research model from Figure 1, the second stage of data analysis, was conducted using partial least squares structural equation modeling (PLS-SEM) approach. It has been deemed an appropriate technique due to the specification of the research model. PLS-SEM approach is a robust technique that handles well both large and small sample sizes. It also does not make any assumptions about the distribution of data, since it is basically a nonparametric method, and works well with relatively complex models (i.e. those that include many indicators and many constructs). In contrast to covariance-based SEM (CB-SEM), PLS-SEM works well with formatively measured constructs. In case of this study, it is proposed that security awareness is in fact a formative type of higher-order construct. Now, CB-SEM approach is also capable of handling formative measures, but it requires the researcher to modify the construct specification. Furthermore, from a pure algorithm perspective, PLS-SEM minimizes the amount of unexplained variance, and is considered generally more efficient than other similar techniques. In addition, the present study is exploratory in nature, which makes any of the confirmatory factor analysis methods less applicable to its context (Hair, Hult, Ringle, & Sarstedt, 2014).

CHAPTER 4

DATA ANALYSIS AND RESULTS

This data analysis and results of the current study are presented in this chapter. It is organized in two main sections. First, a detailed analysis of the phishing experiment is conducted using multiple discriminant analysis method (MDA). Following Ho (2014) and Hair et al. (2010), it organized as follows: (1) characteristics of the employees of the municipality; (2) estimation of the discriminant function; (3) assessment of predictive accuracy along with the classification matrices; and (4) interpretation of the discriminant function; and (6) validation of the results. All of the demographic data were analyzed as categorical variables. Therefore, employee demographic information was not tested for normality assumptions.

Second, the analysis of the research model is presented based on the results obtained from the survey instrument. This study implements partial least squares structural equation modeling (PLS-SEM) approach for analyzing the survey data and testing the research model. The author has used SmartPLS software package to perform the analysis (Ringle, Wende, & Will, 2005). Following the guidelines established by Hair et al. (2014), this part of data analysis is organized in the following sections: (1) data collection and response rate; (2) the analysis of non-response bias; (3) sample characteristics; (4) the evaluation of the measurement model; (4a) evaluation of the reflective measurement model including internal consistency, indicator reliability, convergent validity, and discriminant validity; (4b) the evaluation of the formative measurement model (since security awareness is proposed to be a second-order formative construct) including convergent validity, diagnostics of collinearity among the indicators, and the significance and relevance of outer weights; and (5) the evaluation of the structural model including the analysis of coefficients of determination (R^2), predictive relevance, size and significance of path coefficients, f^2 effect sizes, q^2 effect sizes, and analysis of heterogeneity.

Phishing Experiment

The profiles of the municipality's employees are included in Table 3. The demographic information is based on what the municipality was willing to share with the researcher. This information served as basis for conducting MDA. Overall, the target organization is fairly homogenous in terms of the employee's ethnicity (79% of white ethnical background), employment status (84% employed as full-time regular workers), postal area in which they live (84% living locally in a densely populated metropolitan area), and FLSA exemption status (80% non-exempt). Other characteristics appear to be more differentiated across the employee population. Therefore, MDA approach is appropriate to examine the data.

Table 3

Employee Demographic Information

Variable	Category	Frequency	Percentage
Gender	Male	963	67%
	Female	467	33%
Ethnicity	White	1123	79%
	Black	100	7%
	Hispanic	170	12%
	American Indian / Alaskan Native	9	1%
	Asian / Pacific Islander	17	1%
	Two or More Races	11	1%
Age	20 or less	62	4%
	between 21 and 25	125	9%
	between 26 and 30	134	9%
	between 31 and 35	163	11%
	between 36 and 40	197	14%
	between 41 and 45	212	15%
	between 46 and 50	181	13%
	between 51 and 55	131	9%

(table continues)

Table 3 *(continued)*

Variable	Category	Frequency	Percentage
	between 56 and 60	120	8%
	between 61 and 65	61	4%
	above 65	44	3%
Work Experience (with the municipality)	5 or less	523	37%
	between 6 and 10	307	21%
	between 11 and 15	274	19%
	between 16 and 20	138	10%
	between 21 and 25	90	6%
	between 26 and 30	66	5%
	above 30	32	2%
Marital Status	Single	796	56%
	Married	634	44%
Annual Salary (in thousands)	$20 or less	140	10%
	between $21 and $30	134	9%
	between $31 and $40	281	20%
	between $41 and $50	283	20%
	between $51 and $60	174	12%
	between $61 and $70	185	13%
	between $71 and $80	108	8%
	between $81 and $90	54	4%
	between $91 and $100	27	2%
	above $100	44	3%
Budget Unit	General Fund	715	50%
	Solid Waste	100	7%
	Waste Water	96	7%
	Technology Services	27	2%
	Recreation Fund	67	5%
	Water Fund	147	10%
	Electric Fund	131	9%
	Aquatic Center Fund	80	6%
	Street Improvement Fund	29	2%
	Fleet	20	1%
	Airport	2	0%
	Risk Retention	5	0%
	Materials Management	11	1%
Employment Status	Full time Regular	1195	84%
	Part-time Regular	202	14%
	Full-time Temporary	16	1%
	Part-time Temporary	17	1%
Fair Labor Standards Act (FLSA) Exemption	Yes	288	20%
	No	1142	80%
Employee Home ZIP prefix	750XX	154	11%
	751XX	9	1%
	752XX	9	1%
	754XX	8	1%
	760XX	29	2%
	761XX	23	2%
	762XX	1198	84%

As mentioned in the methodology section, the municipality has experienced increased number of phishing attacks at their infrastructure. Before launching the training program, the organization was interested in finding out whether some groups of individuals are more vulnerable to phishing than others. The phishing experiment included two types of emails, regular phishing and spear-phishing messages. These fake messages were sent to a total 1430 employees of the municipality. The number of clicks on the fake hyperlinks for both attacks is presented in Table 4. Several individuals have attempted to click on a hyperlink several times. This is most likely due to the fact that the links did not take them to the destination they had initially expected. Approximately 2.7% of the employees fell victim to the message containing a fake Amazon.com gift card redemption code. This ratio is marginally higher than a typical ratio for a regular phishing email. In contrast, the spear-phishing message yielded a response rate of approximately 16.5%. Interestingly, industry experts estimate that spear-phishing attack success rate is on average four to five times higher than regular phishing (Hong, 2012). Thus, the results of the spear-phishing attack should be of a serious concern to the municipality's IT management. It should also be mentioned that the spear-phishing email content has been designed based on the information that was publicly available online. Additionally, in a real world situation, the potential attacker would also have no difficulties harvesting the employee email addresses as vast majority of them is available on the municipality's website. On the other hand, the author did not collect any personal information through the phishing links. The employees were only tested if they would click on a hyperlink in a fake message. It was not tested whether they would actually disclose any personal information on the phishing website, per the request of the municipality's officials.

Table 4

Phishing Experiment Statistics

Phish Type	**Unique Clicks**	**Total Clicks**
Regular phishing (i.e., Amazon gift card)	39	76
Spear-phishing (i.e., email from IT admin)	236	338
Total	**275**	**414**

MDA as one of the dependence multivariate techniques relies on meeting certain assumptions. The dataset of employee demographic information used for the analysis of the results of the phishing experiment contains only categorical variables. Hence, it is not tested for normality assumptions. In addition, even though the analysis of potential outliers could improve the overall results of the analysis; this step has also been bypassed, since the demographic information contains information about the whole employee population.

MDA method has been employed using SPSS 21 software package. All the matrices for calculation were calculated from within-groups correlation, and the prior probabilities for the purpose of classification analysis were determined from group sizes. Since the municipality's IT management was interested in finding whether there are any characteristics that could help isolate the individuals prone to phishing, a stepwise method was selected to analyze the demographic information with regards to potential phishing victimization. The final results of the discriminant analysis procedure are presented in Tables 5-8.

The assumption of homogeneity of variance-covariance matrices is tested with Box's M test of equality of covariance matrices. The results indicate that Box's M value of 482.42 (*F* = 17.061) is associated with an alpha level of .000, value of which indicates a violation of the assumption of equality of covariance matrices (see Table 5). However, if the group sizes are unequal (1166 and 264 in this particular case) and the number of independent variables is fairly large, then Box's M test should not be used. Instead, one should use Pillai's criterion to evaluate multivariate significance (Tabachnick & Fidell, 2001). It is considered a reliable multivariate measure, as it offers good protection against Type I errors. Pillai's trace value is equal to .055 (*F* = 11.875) and is significant at .000. Therefore, it was determined that is was possible to proceed with the interpretation of the discriminant function (Hair et al., 2010).

Table 5

Test of Homogeneity of Variance-Covariance Matrices

Log Determinants		
Behavior (0 – not phished, 1 – phished)	**Rank**	**Log Determinant**
0	7	-17.184
1	7	-16.379
Pooled within-groups	7	-16.698
The ranks and natural logarithms of determinants printed are those of the group covariance matrices.		
Test Results		
Box's M		482.42
F	Approx.	17.061
	df1	28
	df2	799024.391
	Sig.	.000
Tests null hypothesis of equal population covariance matrices.		

The next step in the analysis is the interpretation of the test of equality of group means. Based on the stepwise procedure seven variables have been determined to provide significant group differences that are important in discriminating between individuals prone to phishing attacks and those who are expected to protect organizational assets, and thus comply with the requirements of the information security policy. The stepwise procedure was based on Mahalanobis D^2. This procedure is based on generalized Euclidean distance that adjusts for unequal variances. It is also considered appropriate if the number of predictors is large, because it does not affect the dimensionality of the independent variables. It also provides a maximal use of information in the stepwise procedure (Hair et al., 2010). Based on the procedure seven variables were identified as those with potential discriminating power. The results are included in Table 6.

Table 6

Stepwise Statistics and Wilk's Lambda

Step	**Entered**	**Min. *D²***						**Wilk's Lambda**
		Statistic	**Between Groups**	**Exact *F***				
				Statistic	***df1***	***df2***	***Sig.***	
1	Full-time regular	0.148	0 and 1	31.883	1	1428	.000	0.978
2	Salary between $91k and $100k	0.217	0 and 1	23.346	2	1427	.000	0.968
3	Gender Male	0.293	0 and 1	21.001	3	1426	.000	0.958
4	Ethnicity Hispanic	0.329	0 and 1	17.66	4	1425	.000	0.953
5	Age between 31 and 35	0.349	0 and 1	14.981	5	1424	.000	0.950
6	ZIP 762XX	0.369	0 and 1	13.182	6	1423	.000	0.947
7	Electric Fund Budget Unit	0.388	0 and 1	11.875	7	1422	.000	0.945

In general, the primary objective of multiple discriminant analysis is to produce a combination of predictor (independent) variables that maximally separate groups of individuals from each other. Since in this study there are only two groups in the analysis (i.e., those who clicked on a hyperlink in a phishing message, and those who did not), MDA produces only one discriminant function. The canonical discriminant function coefficients are presented in Table 7. Overall, the discriminant function is highly significant based on the chi-square test (χ^2 = 80.927, *df* = 7) of the function's Wilk's Lambda (.945). In addition the discriminant function yields canonical correlation of .235 which explains 5.5% of the variance in phishing behavior. The discriminant function coefficients represent the relative contribution of each respective variable to the discriminant function. Those with larger absolute values contribute more to the discriminating power of the function. On the other hand, those with smaller values contribute less. Their interpretation is similar to the interpretation of beta weights in multiple regression (Hair et al., 2010; Ho, 2014). Similarly to regression, the sign of the weight denotes whether the coefficient makes a positive or a negative contribution to the function. The results show that males, of Hispanic ethnicity, who live in a densely populated area (ZIP code 762XX) were less likely to fall victim of the phishing email. In contrast, individuals aged between 31 and 35 years old, employed as full-time regulars, with an annual salary ranging between $91k and $100k were more prone to being victimized by a phishing email. In addition, it also appears that employees of one of the business units (i.e., Electric Fund) were also more likely to fall victim to phishing attacks than the employees working in other business units.

Table 7

Standardized Canonical Discriminant Function Coefficients and Structure Matrix

	Weight	**Loading**
Gender Male	-0.506	-0.235
Ethnicity Hispanic	-0.316	-0.286
Age between 31 and 35	0.224	0.233
Salary between $91k and $100k	0.449	0.442
Electric Fund Budget Unit	0.226	0.306
Full-time regular	0.683	0.618
ZIP 762XX	-0.238	-0.206

Unfortunately, discriminant function coefficients are subject to the same criticisms as beta weights in multiple regression analysis (e.g., multicollinearity). Therefore, it is often advised to investigate the discriminant loadings (structure correlations) from the structure matrix produced by MDA output. The discriminant loading explains the variance shared by the independent variables with the discriminant function. It is estimated that variables with loadings >= ± .30 should be considered as substantive (Ho, 2014). Under this criterion only three variables would be taken into consideration: full-time regular employment (.618), annual salary between $91k and $100k, and Electric Fund business unit. On the hand, the remaining four variables have loadings lower than .30 (i.e., gender, Hispanic ethnicity, ZIP code 762XX, and age between 31 and 35). Using the stepwise procedure may prevent other variables from entering the equation to account for multicollinearity issues. Hence, if multicollinearity was not an issue, individuals with an annual salary below $20k who are employed part-time by the Aquatic Center business unit aged 20 years old or less would also be present in the discriminant function with loadings above 0.30. They would also be less likely to fall victim to phishing scam. Since the discriminant loadings are not very high for the four variables mentioned above, it is also useful to examine the partial *F* values (Table 6) associated with each variable, especially when the discriminant function is obtained through a stepwise method (Hair et al., 2010). Large *F* values indicate greater discriminatory power. Therefore, despite having their loadings slightly below the recommended threshold, the four variables related to gender, ethnicity, age, and ZIP code were retained in the final model because their partial F values were higher than the partial *F* value associated with Electric Fund business unit. Overall, the results should be treated with caution, as it appears the model is not very strong. One possible explanation is that the two groups under analysis (i.e., phished vs. not phished) were unbalanced, thus weakening the predictive power of the discriminant function.

Table 8

Classification Results

			Predicted Group Membership		
		Group	**Not-phished**	**Phished**	**Total**
Original	Count	Not-phished	716	450	1166
		Phished	99	165	264
	%	Not-phished	61.4	38.6	100
		Phished	37.5	62.5	100
Cross-validated	Count	Not-phished	716	450	1166
		Phished	101	163	264
	%	Not-phished	61.4	38.6	100
		Phished	38.3	61.7	100

61.6% of original grouped cases correctly classified.
Cross validation is done only for those cases in the analysis. In cross validation, each case is classified by the functions derived from all cases other than that case.
61.5% of cross-validated grouped cases correctly classified.

The final steps in the analysis of the discriminant function include the assessment of the predictive accuracy of the discriminant function, as well as the assessment of the classification accuracy. Both of these steps are required because previous tests, while useful for estimation of the significance of the model, do not inform the researcher about the function’s predictive power. The discriminant function’s level of significance is not the indicator of its ability to discriminate between the two groups (i.e., phished vs. non-phished) (Hair et al., 2010). Investigation of the classification results (Table 8) reveals that 61.6% of the cases were correctly classified by the discriminant function. In case of particular groups, that is phished and not-phished individuals, the ratios have similar values 62.5% and 61.4% respectively.

The best way to examine the predictive power of the discriminant function is to compare it with a chance model. Press’s *Q* statistic is a measure that compares the number of correct classifications with the total sample size and the number of groups (Hair et al., 2010). Its calculated value is compared with the chi-square critical value of 6.63 with 1 degree of freedom. If *Q* exceeds the critical value then it can be assumed that the predictive accuracy of the model is greater than that expected by chance. In this study, Press's *Q* = 77.08, which is greater than the critical value. Consequently, the predictive power of the discriminant function determining if a person is likely to get phished is significantly better than chance. However, this test is sensitive to sample size, with large samples being more likely to show significance. As a rule of thumb, classification accuracy should be at least 25% greater than that achieved by chance. Following this rule, the minimum expected hit ratio for this research should be at least 62.5%. The classification results from Table 8 report that the discriminant function achieves accuracy of 61.6%. This is slightly below the recommended threshold. However, it has to be remembered that the groups are highly unbalanced which could affect the overall results.

The overall results of the phishing reveal significant differences in demographic characteristics among the phished and not phished groups of the municipality's employees.

Survey Instrument Analysis

The survey instrument was administered through Qualtrics online survey engine. A personalized hyperlink containing a MD5 hash calculated for each individual email address was sent out to each of 1430 employees. The hash portion of the URL was extracted once a person started answering to the questionnaire. This way, the researcher was able to match the individuals with the results of the phishing experiment. Overall, 359 individuals participated in the survey, yielding a response rate of 25.1%. The participation in the survey was voluntary. Out of the total 359 responses, 172 have been used in the final analysis. The remaining ones were discarded because the participants either did not finish the survey, or they answered all of the questions in less than two minutes. Also, a quick analysis of the respondents revealed that 55 of them have fallen victim to the phishing experiment, while 117 have not. Overall, the response rate should be thought of as relatively high, especially that the participation was voluntary, and that the survey instrument was fairly long. The participants have been informed about the goals of the study, as well as future practical implications derived from the study's findings. Furthermore, the participants were informed about the importance of the study for the organization itself and the local community.

The next step in the analysis is the assessment of non-response bias. In this study, the researcher has collected demographic information for every employee of the municipality. Furthermore, each potential respondent was assigned a unique identifier based on MD5 hashing function applied to each individual email address. Consequently, it was possible to identify each individual who either fell victim to the phishing experiment or who participated in the study's questionnaire. Therefore it was possible to verify whether the sample of survey participant was representative of the municipality's employee population.

Typically, when analyzing non-response bias, one would compare early responders with late responders. However, in this particular situation it was possible to address the issue of representativeness of the sample. Appendix B depicts the comparison between individuals who participated in the survey and the overall population of the municipality's employees. The independent samples test was performed using SPSS 21. The overall results indicate that the sample can be considered representative of the population. The few occasions where the results indicate that the two groups (i.e., survey participants and employee population) are significantly different indicate that the survey was not completed by part-time employees with the annual salary below $20k who are paid from Recreation Funds. However, this has been deemed as not a significant issue, since the majority of individuals are employed full-time. At the other end of the spectrum, individuals with the annual salary over $100k who are FLSA exempt have participated in the survey in a large percent. These individuals are most likely the decision-makers who are interested in designing and implementing effective security awareness education and training programs throughout the whole municipality. Therefore, they might understand the importance of security awareness for the protection of organizational assets more than other employees. Ergo, higher participation rate from these individuals. Finally, employees of Hispanic origin were underrepresented in this study. At the same time however, the phishing experiment has shown that these individuals are less prone to phishing attacks. Consequently, it is possible that the final results of the research model could have possibly resulted in more significant relationships for the employees who were not victimized by the phishing messages. Based on the above, it has been determined that the sample is representative of the municipality's employee population.

Measurement Model Evaluation – Stage 1

The research model in this study has been evaluated with SmartPLS 2.0 software package (Ringle et al., 2005). Model estimation in PLS-SEM is a two-step process. Measurement models are used to test the relationship between the indicators and the constructs. Structural model evaluation, on the other hand, examines the relationships between the constructs. In contrast to CB-SEM, goodness-of-fit criterion is not available in PLS-SEM methods. Unlike CB-SEM, PLS-SEM is focused on the discrepancies between the observed or approximated values of the dependent variables and the values predicted by the model under research. Consequently, when using PLS-SEM approach a researcher is focused on the model's predictive capabilities in order to estimate its quality (Hair et al., 2014).

The first step in discussing PLS-SEM models is to evaluate the measurement model in terms of its constructs' reliability and validity. Also, when examining measurement models, it needs be clearly stated whether the constructs are measured reflectively or formatively. In case of this study, security awareness (SA) is a higher-order formative construct. However, all of the lower-order constructs that are the hypothesized components of SA are measured reflectively as it described in Table 2. Therefore, the evaluation of the measurement model was conducted in two stages.

Table 9

Analysis of Reliability and Validity for Stage 1 Measurement Model

	AVE	***CR***	***R²***	**Alpha**	**ATT**	**COST**	**EFFECT**	**EXP**	**INT**	**IIS**	**RESP**	**REW**	**SAN**	**SE**	**SEV**	**SUSC**
ATT	0.93	0.98	0.26	0.98	**0.97**											
COST	0.69	0.81	0.21	0.56	-0.28	**0.83**										
EFFECT	0.74	0.89	0.36	0.82	0.44	-0.29	**0.86**									
EXP	0.81	0.93	0.00	0.88	0.22	-0.17	0.57	**0.90**								
INT	0.98	0.99	0.61	0.99	0.77	-0.25	0.43	0.16	**0.99**							
IIS	0.60	0.88	0.00	0.83	0.43	-0.34	0.39	0.35	0.36	**0.77**						
RESP	0.69	0.87	0.21	0.78	-0.22	0.38	-0.35	-0.39	-0.29	-0.30	**0.83**					
REW	0.78	0.91	0.00	0.86	0.12	0.22	0.00	0.02	0.04	0.22	0.12	**0.88**				
SAN	0.79	0.92	0.00	0.87	0.25	-0.13	0.17	0.26	0.22	0.31	-0.09	0.29	**0.89**			
SE	0.77	0.93	0.33	0.90	0.15	-0.02	0.58	0.57	0.18	0.18	-0.19	0.06	0.11	**0.87**		
SEV	0.76	0.93	0.12	0.89	0.40	-0.15	0.37	0.17	0.38	0.35	-0.17	0.08	0.14	-0.01	**0.87**	
SUSC	0.75	0.92	0.09	0.89	0.14	0.03	-0.04	0.08	0.05	0.26	-0.03	0.20	0.17	-0.24	0.50	**0.87**

In Stage 1, the measurement model including all of SA's underlying constructs and indicators was evaluated for internal consistency, individual indicator reliability, and average variance extracted (AVE). Typically, internal consistency is the first criterion being examined. Traditionally, Cronbach's alpha is the standard measurement of constructs reliability. However, due to its limitations that are discussed elsewhere, it is more appropriate to use composite reliability (Hair et al., 2014). Examination of composite reliability values in Table 9 reveals that all of them are above recommended threshold of 0.7. However composite reliability scores for ATT and INT are above 0.95, which could indicate that respective indicator variables could be measuring the same phenomenon, which could potentially impose a threat to the instrument's validity (Hair et al., 2014). Consequently, composite reliability scores above the recommended 0.95 threshold may negatively affect the instrument's content validity (Rossiter, 2002), as well as inflate error term correlations (Drolet & Morrison, 2001). On the other hand, the items for both ATT and INT constructs have been adapted from previously validated scales (Bulgurcu et al., 2010). In addition they did not yield any potential issues in the pilot study's results where their reliability scores were around 0.90, which was within the recommended interval for reliability scores. Therefore, it is assumed that the measurement model meets the criteria for internal consistency reliability.

Having established the reliability of the instrument, the next step in the measurement model evaluation is to assess its validity. Convergent validity is an indicator of how well a measure correlates with alternative measures of the same construct. Consequently, measurements of the same construct should share a large proportion of variance between each other. The two most common measures of convergent validity are the outer loadings and AVE (Tables 9 and 10). Outer loadings are interpreted in the following way; higher loadings on a given construct indicate that the associated indicators have a lot in common which is captured by the nature of the overarching construct. As a rule of thumb, outer loadings should be 0.708 or higher. In this study, the only indicator that does not meet the recommended threshold is SEV_4 that has an outer loading of 0.672 on SEV construct. In such cases, one should examine if the removal of the indicator from the model would have an impact on AVE and composite reliability scores. Removing SEV_4 did not yield significant improvements on either of the above; therefore the item was retained for further analysis, especially that its outer loading was just marginally lower than the recommended criterion. Another common measure for establishing convergent validity is AVE, which can be defined as the grand mean value of the squared loadings of the indicators associated with the construct (Hair et al., 2014). It is also equivalent to the communality of a variable. The common criterion is that AVE values for each constructs should be above 0.50, which indicates that it explains majority of variance in its indicators. AVE values are reported in Table 6 with all of them exceeding the recommended minimum score. Therefore, the convergent validity of the instrument is confirmed.

Finally, discriminant validity is the extent to which a given construct differentiates itself from other constructs in the model. As result, constructs having discriminant validity are assumed to be unique and capture phenomena not captured by other constructs in the model. The two most widely used criteria for establishing discriminant validity are the cross-loadings of the indicators and the Fornell-Larcker criterion. The former criterion assumes that indicator’s outer loadings should be greater than all of its cross loadings on other construct. The examination of the cross loadings information in Table 7 reveals cross loadings are not an issue in this study, since all of the indicators have higher outer loadings on their expected constructs than they have cross-loadings on other constructs. Fornell-Larcker criterion, the second measure of discriminant validity, states that the square root of each construct's AVE should be greater than its highest correlation with any other construct (Fornell & Larcker, 1981; Hair et al., 2014). In case of this study, the square roots of AVE for each of the constructs included in the research model are presented in the diagonal of the correlation matrix in Table 6. Since all square roots of the AVEs are greater than the construct correlations with other constructs, the results provide sufficient support for establishing discriminant validity.

Table 10

Outer Loadings (in Bold) and Cross Loadings for Stage 1 Measurement Model

	ATT	COST	EFFECT	EXP	INT	IIS	RESP	REW	SAN	SE	SEV	SUSC
ATT_1	**0.962**	-0.288	0.458	0.239	0.790	0.422	-0.268	0.094	0.273	0.192	0.360	0.089
ATT_2	**0.971**	-0.259	0.417	0.220	0.681	0.407	-0.182	0.121	0.237	0.113	0.407	0.168
ATT_3	**0.972**	-0.285	0.415	0.206	0.788	0.404	-0.235	0.116	0.265	0.141	0.374	0.126
ATT_4	**0.961**	-0.253	0.390	0.202	0.696	0.422	-0.168	0.142	0.181	0.112	0.404	0.154
INT_1	0.770	-0.243	0.454	0.170	**0.984**	0.374	-0.291	0.073	0.246	0.190	0.360	0.034
INT_2	0.754	-0.258	0.401	0.151	**0.989**	0.335	-0.283	0.030	0.211	0.151	0.378	0.051
INT_3	0.749	-0.251	0.418	0.158	**0.992**	0.362	-0.289	0.030	0.192	0.185	0.375	0.061
IIS_1	0.329	-0.307	0.260	0.253	0.347	**0.809**	-0.274	0.161	0.345	0.082	0.279	0.184
IIS_2	0.378	-0.135	0.204	0.136	0.312	**0.759**	-0.149	0.246	0.204	0.014	0.268	0.312
IIS_3	0.245	-0.325	0.355	0.275	0.261	**0.849**	-0.217	0.156	0.231	0.146	0.242	0.179
IIS_4	0.284	-0.212	0.383	0.462	0.143	**0.718**	-0.293	0.173	0.180	0.339	0.192	0.118
IIS_5	0.427	-0.295	0.279	0.215	0.332	**0.730**	-0.201	0.123	0.214	0.092	0.350	0.222
COST_1	-0.114	**0.745**	-0.156	-0.068	-0.058	-0.200	0.131	0.254	-0.037	-0.047	0.002	0.097
COST_2	-0.315	**0.907**	-0.299	-0.197	-0.312	-0.338	0.436	0.149	-0.159	0.000	-0.205	-0.026
EFFECT_1	0.324	-0.255	**0.927**	0.550	0.342	0.339	-0.326	-0.014	0.138	0.542	0.278	-0.075
EFFECT_2	0.276	-0.241	**0.895**	0.545	0.267	0.297	-0.263	-0.004	0.100	0.592	0.192	-0.144
EFFECT_3	0.523	-0.248	**0.749**	0.359	0.498	0.358	-0.321	0.011	0.192	0.355	0.476	0.107
EXP_1	0.146	-0.204	0.466	**0.845**	0.130	0.362	-0.381	0.015	0.312	0.434	0.123	0.040
EXP_2	0.199	-0.099	0.501	**0.908**	0.105	0.270	-0.298	0.026	0.131	0.550	0.151	0.056
EXP_3	0.252	-0.170	0.553	**0.939**	0.195	0.316	-0.383	0.022	0.259	0.551	0.176	0.104
SEV_1	0.278	-0.193	0.248	0.184	0.270	0.352	-0.156	0.034	0.131	-0.012	**0.864**	0.416
SEV_2	0.329	-0.086	0.331	0.157	0.336	0.251	-0.124	0.044	0.089	-0.006	**0.932**	0.503
SEV_3	0.408	-0.170	0.354	0.111	0.407	0.319	-0.145	0.042	0.084	-0.034	**0.943**	0.430

(table continues)

Table 10 *(continued)*

	ATT	COST	EFFECT	EXP	INT	IIS	RESP	REW	SAN	SE	SEV	SUSC
SEV_4	0.374	-0.062	0.349	0.138	0.289	0.283	-0.161	0.166	0.193	0.040	**0.735**	0.403
SUSC_1	0.076	0.044	-0.046	0.126	-0.031	0.231	-0.054	0.180	0.138	-0.170	0.366	**0.829**
SUSC_2	0.123	0.038	-0.074	0.020	0.065	0.207	0.012	0.158	0.083	-0.247	0.454	**0.863**
SUSC_3	0.098	-0.004	-0.044	0.047	0.047	0.190	-0.062	0.146	0.164	-0.226	0.445	**0.892**
SUSC_4	0.170	0.014	0.002	0.069	0.081	0.259	-0.009	0.198	0.191	-0.181	0.474	**0.885**
RESP_1	-0.236	0.399	-0.203	-0.183	-0.314	-0.251	**0.853**	0.098	-0.075	0.017	-0.176	-0.031
RESP_2	-0.223	0.391	-0.181	-0.194	-0.324	-0.229	**0.847**	0.154	-0.028	-0.013	-0.197	-0.050
RESP_3	-0.117	0.186	-0.442	-0.527	-0.122	-0.250	**0.788**	0.061	-0.113	-0.387	-0.066	-0.005
REW_2	0.148	0.154	0.050	0.106	0.103	0.305	0.057	**0.817**	0.316	0.099	0.128	0.211
REW_3	0.079	0.243	-0.034	-0.056	0.005	0.131	0.141	**0.941**	0.201	0.016	0.043	0.152
REW_4	0.104	0.191	-0.016	0.028	0.021	0.159	0.116	**0.891**	0.260	0.042	0.047	0.169
SE_1	0.143	-0.016	0.517	0.472	0.172	0.168	-0.190	0.048	0.063	**0.865**	0.002	-0.196
SE_2	0.089	-0.016	0.457	0.500	0.110	0.134	-0.125	0.053	0.129	**0.867**	-0.038	-0.189
SE_3	0.148	-0.034	0.557	0.525	0.200	0.180	-0.217	0.067	0.093	**0.886**	0.010	-0.222
SE_4	0.128	-0.009	0.489	0.503	0.135	0.133	-0.120	0.026	0.113	**0.881**	0.006	-0.215
SAN_1	0.226	-0.131	0.188	0.213	0.229	0.302	-0.107	0.220	**0.899**	0.086	0.117	0.158
SAN_2	0.254	-0.163	0.155	0.197	0.207	0.244	-0.087	0.156	**0.877**	0.134	0.078	0.104
SAN_3	0.198	-0.078	0.109	0.266	0.156	0.261	-0.055	0.349	**0.887**	0.094	0.159	0.172

Measurement Model Evaluation – Stage 2

The evaluation of the measurement model has been conducted in two stages because SA was conceptualized as a second-order formative construct composed of SEV, SUSC, COST, RESP, SE, and EFFECT. A two-stage repeated indicator approach mode B (Becker, Klein, & Wetzels, 2012) was used to obtain latent variable scores for the hypothesized measures of SA. In case of this study SA as a second-order construct also has other antecedents than the six lower-order constructs mentioned above. A single stage repeated indicator approach would not be applicable in this context, because most of the variance in SA would be explained by its lower-order formative constructs (i.e., R^2 would approximately reach the value of 1.0). As a result, the other paths in the structural model pointing to the higher-order construct would be insignificant. In such situations, it is strongly recommended to apply a mixture of the repeated indicator approach and the usage of latent variable scores (Becker et al., 2012; Hair et al., 2014;

Henseler & Chin, 2010). This method uses repeated indicator approach to obtain latent variable scores for the lower-order constructs, which then in turn serve as the manifest variables on the measurement model for the higher-order construct. Consequently, such a nomological net allows other constructs to be used as antecedents of the higher-order construct. This method was especially important for the context of this study, because the researcher was interested in the investigation of the antecedents of security awareness, as well as their predictive power.

After calculating latent variable scores for the components of SA in Stage 1, these values were used as manifest variables for SA represented as a formative construct. The measurement model was then reevaluated for its reliability and validity. In addition, SA as a formative construct was assessed for collinearity issues, as well as for the significance and the relevance of the formative indicators. It is also strongly advised to conduct redundancy analysis to assess the convergent validity of the formative construct (Chin, 1998). In essence, redundancy analysis proposes to use a formatively measured construct as an exogenous variable in order to predict an endogenous variable operationalized through one or more reflective measures (Hair et al., 2014). The interpretation of the results is as follows; the strength of the path coefficient joining the two latent variables is an indicator of validity of the set of formative indicators. For convergent validity to be established the path coefficient value should be of at least 0.80, ideally more than 0.90. The author has used the reflective measures for organizational security awareness. This information was collected in the survey instrument along with the measure for personal security awareness that was the primary focus of the study. Redundancy analysis yielded a path coefficient of 0.947 between the exogenous formatively measured personal SA and the endogenous reflectively measured organizational SA. This value translates to an R^2

value of 0.897 that provides support for the convergent validity of second-order formative SA for personal threats.

The next step in the evaluation of the formatively measured variables is to evaluate them for collinearity issues. Computing the tolerance (i.e., the amount of variance of one formative indicator not explained by other indicators) is a common method of assessing multicollinearity problems. Also, variance inflation factor (VIF) is another criterion commonly implemented for the detection of collinearity issues. Both measures are closely related to each other, as VIF is nothing else than the reciprocal of the tolerance. The results of the tests for both tolerance and VIF are included in Table 11. In both cases the values of tolerance and VIF for each of the formative indicators of SA are above recommended threshold of 0.20 for tolerance, and below recommended threshold of 5.0 for VIF. Therefore, it is concluded that collinearity is not an issue for the six formative indicators of SA.

Table 11

Examination of Collinearity among the Formative Measures for SA

	Tolerance	**VIF**
COST	0.795	1.258
EFFECT	0.456	2.194
RESP	0.787	1.270
SE	0.578	1.730
SEV	0.576	1.737
SUSC	0.671	1.490
Collinearity not an issue:	**if > 0.2**	**if < 5.0**

Assessment of the significance and the relevance of the formative indicators is the final step in the formative measurement model investigation procedure. In this step, it is essential to examine the contribution of each formative indicator to the overarching formative latent variable. A simple method of finding each indicator’s relevance is to investigate their outer weights, and outer loadings if necessary. The outer weight is the result of performing multiple regression, in which the latent variable score for a construct is the dependent variable, and the formative indicators serve as the independent variables. The PLS-SEM method tests if outer weights are significantly different from zero using the bootstrapping procedure. It is advised to use 5000 random subsamples (Hair et al., 2014). However, a non-significant outer weight is not necessarily an indicator of poor measurement quality. Also, it does not indicate that a measurement should be dropped from the model. In such cases, it is advised to evaluate a formative indicator’s absolute contribution to its formative construct. The absolute contribution is contextualized by the formative indicator’s outer loadings. The statistics of the outer weights and outer loadings for the formative indicators of SA are included in Table 12.

Table 12

Assessment of the Significance and Relevance of the Formative Indicators of SA

	Outer Weights			**Outer Loadings**		
	Weight	**STDEV**	**T Statistics**	**Loading**	**STDEV**	**T Statistics**
COST	-0.151	0.106	1.434	-0.433	0.135	3.217
EFFECT	0.571	0.132	4.336	0.898	0.052	17.313
RESP	-0.219	0.106	2.063	-0.564	0.123	4.596
SE	0.224	0.103	2.172	0.556	0.103	5.422
SEV	0.228	0.111	2.055	0.586	0.088	6.658
SUSC	0.180	0.088	2.046	0.220	0.097	2.267

The basic decision process in evaluating whether formative indicators are to be kept in in the model is as follows; if the outer weight is significant, then a given formative indicator is retained in the model. In the present study, all formative indicators have outer weights statistically significant, except COST (*t-value*: 1.434). If the outer weight is not significant, then formative outer loadings should be examined. In case of COST its outer loading of -0.433 is below the recommended threshold of 0.50, but it is significant. Therefore, the indicator is retained in the model, because its inclusion is strongly supported by the theoretical foundations of the present study (Milne et al., 2000; Rogers, 1975), as well as the requirements of the content validity (Hair et al., 2014). Therefore, the formative measurement model was deemed valid, free of multicollinearity issues, and statistically significant in order to be used in the structural model evaluation.

In addition, the remaining reflectively measured latent variables in the Stage 2 model were reevaluated for their internal consistency reliability, convergent validity and discriminant validity. Based on the same criteria that were used in Stage 1, the measurement model in Stage 2 was deemed both reliable and valid to be used in the structural model evaluation. The detailed statistics are included in Tables 13 and 14.

Table 13

Analysis of Reliability and Validity for Stage 2 Measurement Model

	AVE	***CR***	R^2	**Alpha**	**ATT**	**EXP**	**INT**	**ISPA**	**IIS**	**REW**	**SAN**	**SA**
ATT	0.935	0.983	0.267	0.977	**0.967**							
EXP	0.799	0.923	0.000	0.873	0.262	**0.894**						
INT	0.977	0.992	0.604	0.988	0.767	0.227	**0.988**					
ISPA	0.920	0.979	0.000	0.971	0.264	0.642	0.193	**0.959**				
IIS	0.598	0.881	0.000	0.832	0.423	0.409	0.351	0.356	**0.773**			
REW	0.773	0.911	0.025	0.859	0.133	0.082	0.061	0.160	0.246	**0.879**		
SAN	0.791	0.919	0.107	0.869	0.253	0.267	0.220	0.327	0.298	0.297	**0.890**	
SA	0.000	0.000	0.533	0.000	0.488	0.671	0.482	0.560	0.508	0.024	0.223	**formative**

Table 14

Outer Loadings (In Bold) and Cross Loadings for Stage 2 Measurement Model

	ATT	EXP	INT	ISPA	IIS	REW	SAN	SA
ATT_1	**0.963**	0.280	0.790	0.291	0.416	0.109	0.277	0.504
ATT_2	**0.971**	0.259	0.681	0.246	0.404	0.130	0.241	0.465
ATT_3	**0.973**	0.239	0.788	0.258	0.397	0.124	0.268	0.471
ATT_4	**0.961**	0.232	0.696	0.220	0.417	0.156	0.184	0.443
INT_1	0.771	0.248	**0.984**	0.194	0.365	0.086	0.248	0.491
INT_2	0.755	0.205	**0.989**	0.181	0.324	0.047	0.210	0.459
INT_3	0.750	0.220	**0.992**	0.196	0.351	0.046	0.192	0.478
ISPA_1	0.217	0.635	0.159	**0.942**	0.319	0.145	0.346	0.536
ISPA_2	0.221	0.569	0.152	**0.966**	0.302	0.140	0.309	0.518
ISPA_3	0.263	0.617	0.218	**0.971**	0.350	0.138	0.298	0.539
ISPA_4	0.310	0.636	0.209	**0.956**	0.391	0.188	0.301	0.552
IIS_1	0.329	0.274	0.347	0.211	**0.794**	0.188	0.339	0.370
IIS_2	0.378	0.195	0.312	0.168	**0.746**	0.269	0.203	0.290
IIS_3	0.245	0.308	0.261	0.285	**0.850**	0.182	0.225	0.419
IIS_4	0.284	0.492	0.143	0.396	**0.751**	0.194	0.179	0.456
IIS_5	0.427	0.251	0.332	0.264	**0.720**	0.140	0.214	0.388
EXP_1	0.209	**0.836**	0.218	0.532	0.372	0.059	0.351	0.545
EXP_2	0.175	**0.901**	0.102	0.542	0.319	0.061	0.115	0.566
EXP_3	0.306	**0.942**	0.277	0.638	0.403	0.097	0.253	0.676
COST	-0.281	-0.146	-0.253	-0.125	-0.336	0.214	-0.137	**-0.433**
EFFECT	0.435	0.642	0.430	0.509	0.394	0.010	0.167	**0.898**
RESP	-0.223	-0.387	-0.291	-0.367	-0.300	0.109	-0.092	**-0.564**
SE	0.146	0.597	0.178	0.465	0.192	0.069	0.117	**0.556**
SEV	0.398	0.209	0.375	0.171	0.340	0.093	0.135	**0.586**
SUSC	0.137	0.087	0.049	0.146	0.251	0.209	0.164	**0.220**
REW_1	0.148	0.155	0.103	0.176	0.304	**0.883**	0.309	0.082
REW_2	0.079	-0.017	0.005	0.105	0.130	**0.902**	0.190	-0.046
REW_3	0.104	0.026	0.021	0.118	0.160	**0.851**	0.250	-0.013
SAN_1	0.226	0.216	0.229	0.259	0.295	0.243	**0.890**	0.225
SAN_2	0.254	0.208	0.207	0.254	0.240	0.179	**0.903**	0.199
SAN_3	0.198	0.281	0.156	0.352	0.261	0.358	**0.876**	0.174

Structural Model Evaluation

The first step in the structural model evaluation process is to assess it for collinearity issues. It employs the exact same logic that was used to evaluate the formative measurement model. That is the tolerance levels are below 0.20 and VIFs are above 5.00 would indicate significant issues with collinearity between constructs. Per the results presented in Table 15, it was determined that there was no indication of collinearity between the latent variables.

Analysis of the path coefficients is the second step in the structural model evaluation. The path coefficients are obtained from running the PLS-SEM algorithm, and represent the hypothesized relationships among the constructs. The significance of the path coefficients is obtained through the bootstrapping algorithm that produces the standard error for each coefficient. The bootstrapping routine was executed with 172 cases and 5000 subsamples, per the recommendation of Hair et al. (2014). The overall results for the research model are presented in Figure 4.

Table 15

Collinearity Diagnostics for the Structural Model

	Tolerance	**VIF**
ATT	0.373	2.684
EXP	0.434	2.303
INT	0.385	2.596
ISPA	0.524	1.909
IIS	0.642	1.557
REW	0.851	1.174
SAN	0.790	1.265
SA	0.376	2.662
Collinearity not an issue:	**if > 0.20**	**if < 5.00**

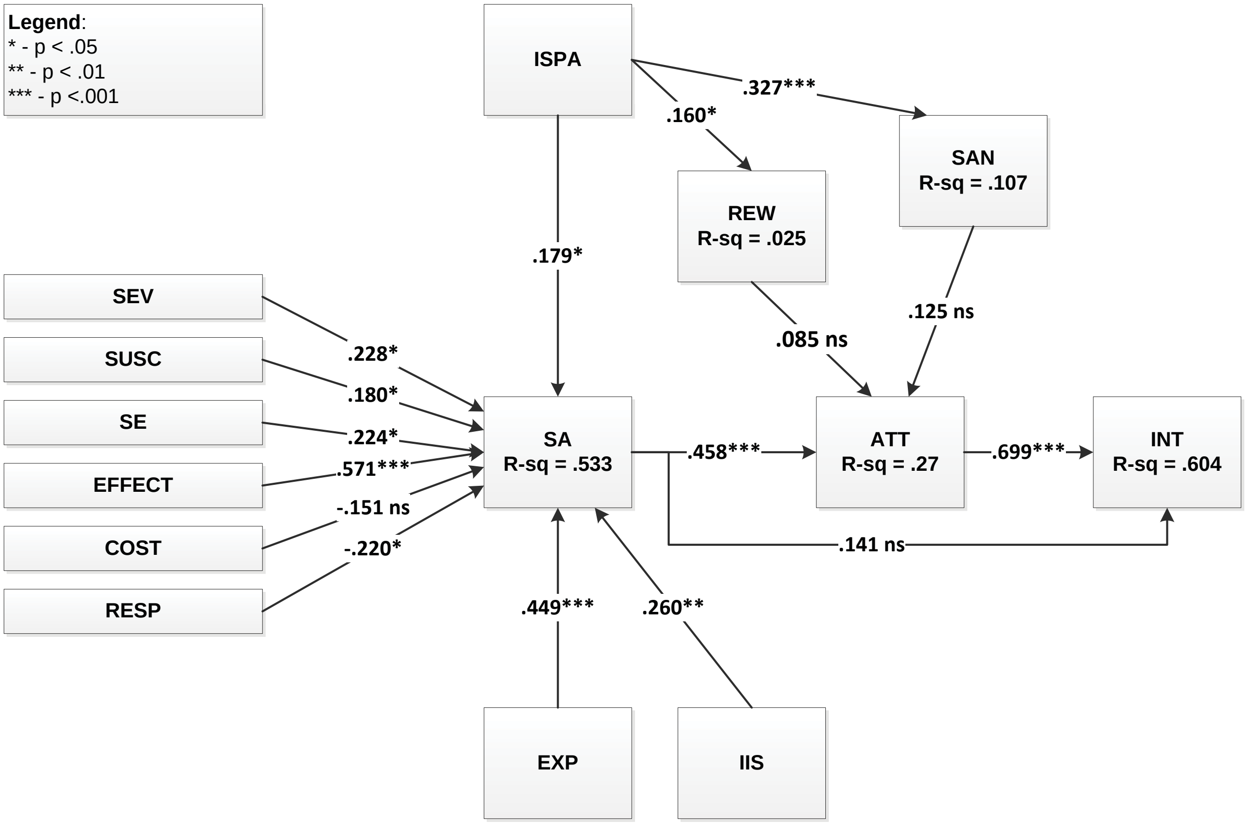


Figure 4. Results of the structural model testing.

The significance and the relevance of the formative SA construct have been discussed in Stage 2 evaluation of the measurement model. EFFECT, RESP, SE, SEV, and SUSC have been found to significantly contribute to the higher-order construct (SA). The outer weight for COST was not significant; however, it was retained in the model because its outer loading was significant as presented in Table 9. It was also an important element of the model from the theoretical perspective. Therefore, removal of COST as a lower-order construct could result in limiting the theoretical value of the research model analysis.

Table 16

Results of Hypothesis Testing

Hypothesis		**Path Coeff.**	**SE**	**T Statistics**	**p-value**	**Supported ?**
H1	Individuals' previous experience with information security threats will positively affect information security awareness.	0.449	0.090	**4.980**	0.000	**Yes**
H2	Individuals' interest to learn about information security threats will positively affect information security awareness.	0.260	0.086	**3.030**	0.003	**Yes**
H3	Individuals' information security policy awareness will positively affect information security awareness.	0.179	0.082	**2.183**	0.030	**Yes**
H4	Information security policy awareness will positively affect knowledge about rewards for compliance.	0.160	0.075	**2.122**	0.035	**Yes**
H5	Information security policy awareness will positively affect knowledge about sanctions for non-compliance.	0.327	0.069	**4.738**	0.000	**Yes**
H6	Information security awareness will positively affect individual's attitude towards compliance with information security policy.	0.458	0.086	**5.361**	0.000	**Yes**
H7	Rewards will positively affect individual's attitude towards compliance with information security policy.	0.085	0.067	1.282	0.202	No
H8	Sanctions will positively affect individual's attitude towards compliance with information security policy.	0.125	0.088	1.423	0.157	No
H9	Attitude will positively affect individual's intention to comply with information security policy.	0.699	0.074	**9.469**	0.000	**Yes**
H10	Security awareness will positively affect individual's intention to comply with information security policy.	0.141	0.077	1.832	0.069	No

The antecedents of awareness (i.e., EXP, IIS, and ISPA) were found to be significantly affecting SA. Thus, the data analysis results provide support for H1, H2, and H3. The study's results also provide support for H4 and H5. That is, information security policy awareness did positively affect the knowledge about rewards for compliance (H4), and the knowledge about sanctions for non-compliance (H5). Contrary to the theorized relationships, the knowledge about rewards and the knowledge about sanctions does not significantly influence individual's attitude towards compliance with information security policy. Thus, H7 and H8 were not supported. Finally, the results provide support for the significant relationship between security awareness and attitude towards compliance with information security policy, and a positive and significant relationship between attitude towards compliance with information security policy and the intention to comply with information security policy. Therefore, H6 and H8 are supported. In contrast, in presence of ATT, the relationship between SA and INT is not significant. Thus, H10 is not supported. In addition, the author has examined the model for the mediating effect of ATT on the relationship between SA and INT. Based on well-established techniques (Baron & Kenny, 1986; Judd & Kenny, 1981), it has been determined that ATT fully mediates the relationship between SA and INT. The summary of the results is included in Table 16.

The next step in the analysis is the examination of the coefficient of determination (i.e., R^2). Overall, the research model explains 60.4% of variance in the intention to comply with organizational security policy. This R^2 value can be interpreted as somewhere between substantial and moderate (Hair et al., 2014; Henseler, Ringle, & Sinkovics, 2009). Also, one of this study's goals was to examine the antecedents of security awareness. EXP, IIS, and ISPA collectively explain 53.3% of variance in SA, all three of them being significant predictors of awareness. In addition, the author has examined the f^2 effect size of the three antecedents of SA on the latent variable. The effect size of EXP on SA was medium, while the effect sizes of both IIS and ISPA were small (Cohen, 1988). The detailed data on the effect size analysis is included in Table 17. Finally, when evaluating the magnitude of R^2 values, it is also advised to apply the criterion of predictive accuracy obtained from Stone-Geisser's Q^2 value (Geisser, 1974; Stone, 1974). The Q^2 values can be calculated and interpreted for endogenous constructs that are measured reflectively only (Hair et al., 2014). Therefore, the statistic was not calculated for SA. However, it has been calculated for ATT and INT yielding values of 0.2349 and 0.5858 which implies that the model has predictive relevance.

Table 17

Analysis of the Effect Size of the Antecedents of Security Awareness

	R^2 excluded	**Effect size**
EXP	0.406	0.27
IIS	0.511	0.05
ISPA	0.507	0.06

Multigroup Analysis and Heterogeneity

Based on the design of the phishing experiment, each individual who participated in the questionnaire was matched with their behavior towards the phishing messages that were sent to the municipality's employees. Consequently, it was possible to compare the two groups of users (i.e., those who did not respond to phishing emails vs. those individuals who did). Because the observation of direct behavior was separated from the self-reported survey instrument, it was possible to control for common method variance that otherwise could have been attributed to issues with using the same measurement instrument (Podsakoff et al., 2003). Multigroup analysis has been performed to analyze the difference between individuals who complied with the organizational information security policy and those who did not. PLS-SEM employs several different techniques for analyzing the differences between groups, collectively falling under the common term of PLS-MGA (Hair et al., 2014), that allow for the comparison of PLS model estimates across different groups of data. In case of this study, a parametric approach to PLS-MGA (Keil, Tan, Wei, Saarinen, & Tuunainen, 2000; Mooi & Sarstedt, 2011) was implemented to analyze the differences between the two aforementioned groups. This method requires knowing the size, path coefficients, and standard errors for both groups. Out of 172 responses used for data analysis, 117 came from individuals who did not fall for the phishing scam and 55 were received from employees who were victimized by the phishing messages. Path coefficients and standard errors were obtained through running the PLS-SEM algorithm and the bootstrapping procedure with 5000 resamples for each group. The results are presented in Table 18.

Table 18

Comparison of PLS Results between Phished and Not Phished Groups

		Phished (N=55)			**Not Phished (N=117)**		
Hypothesis	**Path**	**Path Coeff.**	**SE**	**T Statistics**	**Path Coeff.**	**SE**	**T Statistics**
H1	EXP -> SA	0.417	0.233	1.791	0.488	0.107	4.557
H2	IIS -> SA	0.192	0.191	1.007	0.313	0.103	3.041
H3	ISPA -> SA	0.309	0.240	1.288	0.094	0.111	0.846
H4	ISPA -> REW	0.387	0.123	3.154	0.210	0.192	1.093
H5	ISPA -> SAN	0.417	0.117	3.576	0.299	0.092	3.265
H6	SA -> ATT	0.487	0.322	1.512	0.373	0.095	3.937
H7	REW -> ATT	0.182	0.111	1.648	-0.018	0.090	0.205
H8	SAN -> ATT	-0.014	0.158	0.091	0.297	0.080	3.730
H9	ATT -> INT	0.739	0.108	6.836	0.623	0.078	8.037
H10	SA -> INT	-0.030	0.176	0.171	0.257	0.085	3.026

The size of both groups along with their respective path coefficients and standard errors were used to evaluate whether the variances of parameter estimates are significantly different across groups using Levene’s test. The result of the test determined the appropriate test statistic to be used, as described by Hair et al. (2014). Levene’s test revealed that standard errors in both groups are equal. The results of the PLS-MGA analysis are presented in Table 19.

Table 19

PLS-MGA Results

Path	Path Phished	SE Phished	Path Not Phished	SE Not Phished	T value	p-value
EXP -> SA	0.417	0.233	0.488	0.107	0.320	0.749
IIS -> SA	0.192	0.191	0.313	0.103	7.726	0.000
ISPA -> SA	0.309	0.240	0.094	0.111	12.324	0.000
ISPA -> REW	0.387	0.123	0.210	0.192	6.763	0.000
ISPA -> SAN	0.417	0.117	0.299	0.092	9.008	0.000
SA -> ATT	0.487	0.322	0.373	0.095	6.516	0.000
REW -> ATT	0.182	0.111	-0.018	0.090	15.654	0.000
SAN -> ATT	-0.014	0.158	0.297	0.080	25.383	0.000
ATT -> INT	0.739	0.108	0.623	0.078	10.379	0.000
SA -> INT	-0.030	0.176	0.257	0.085	21.746	0.000

PLS-MGA results revealed that the two groups were significantly different in every dimension except for the path between EXP and SA. However, in this case the true nature of difference between the groups is clouded by relatively small absolute difference between the path coefficients (0.417 and 0.488) in comparison with relatively large standard error values. As a result, the value of the test statistic is deflated. These results should be evaluated with caution since standard errors for the phished group are fairly large in comparison to the path coefficients, and preferably, in conjunction with structural model evaluation for the two groups run separately (see Table 20). In case of individuals who did not click on the phishing email hyperlink, their SA depended on two significant antecedents, i.e., EXP and IIS. In contrast SA levels of the phished group depended only on EXP and it is significant only at 0.1 level. Also, individuals from the not phished group were more interested in learning about information security threats than their colleagues from the phished group. In addition, in case of the phished group, there were no significant relationship between SA and ATT. These individuals formed their attitude towards compliance based on the availability of rewards, with a marginally significant relationship between REW and ATT. Furthermore, phished individuals tend to have stronger connection between ATT and INT. On the other hand, attitudes of the members of the not phished group were also significantly affected by sanctions (significant path between SAN and ATT), which is not the case for their counterparts in the second group.

Table 20

Comparison of Two Structural Models for Phished and Not Phished Groups

		Phished (N=55)				**Not Phished (N=117)**			
Hypothesis	**Path**	**Path Coeff.**	**SE**	**T Statistics**	**Supported?**	**Path Coeff.**	**SE**	**T Statistics**	**Supported?**
H1	EXP -> SA	0.417	0.233	1.791	No	0.488	0.107	**4.557**	**Yes**
H2	IIS -> SA	0.192	0.191	1.007	No	0.313	0.103	**3.041**	**Yes**
H3	ISPA -> SA	0.309	0.240	1.288	No	0.094	0.111	0.846	No
H4	ISPA -> REW	0.387	0.123	**3.154**	**Yes**	0.210	0.192	1.093	No
H5	ISPA -> SAN	0.417	0.117	**3.576**	**Yes**	0.299	0.092	**3.265**	**Yes**
H6	SA -> ATT	0.487	0.322	1.512	No	0.373	0.095	**3.937**	**Yes**
H7	REW -> ATT	0.182	0.111	1.648	No	-0.018	0.090	0.205	No
H8	SAN -> ATT	-0.014	0.158	0.091	No	0.297	0.080	**3.730**	**Yes**
H9	ATT -> INT	0.739	0.108	**6.836**	**Yes**	0.623	0.078	**8.037**	**Yes**
H10	SA -> INT	-0.030	0.176	0.171	No	0.257	0.085	**3.026**	**Yes**

Overall, the two groups under comparison were different which revealed interesting insights about the employee population. Therefore, the formative measurement for SA has been analyzed for both groups (Table 21). In case of phished individuals, none of the weights was significantly contributing to the SA formative construct. In addition, some of the outer loadings were not significant as well. Therefore, it can be questioned whether phished individuals actually have SA. On the other hand, only two weights (EFFECT and SEV) were significantly contributing to the formative SA construct for the not-phished group. However, the outer loadings for the not phished group were all significant except SUSC. Consequently, it appears that the not phished group actually has some levels of SA, just as is it posited in the present study.

Table 21

Assessment of the Significance and Relevance of Formative Indicators of SA between Groups

Phished Outer Weights				**Not Phished Outer Weights**			
	Weight	**SE**	**T Statistics**		**Weight**	**SE**	**T Statistics**
COST	-0.098	0.181	0.540	COST	-0.161	0.109	1.480
EFFECT	0.425	0.303	1.402	EFFECT	0.568	0.139	4.078
RESP	-0.445	0.349	1.276	RESP	-0.158	0.099	1.593
SE	0.343	0.229	1.498	SE	0.169	0.101	1.677
SEV	-0.088	0.247	0.357	SEV	0.299	0.119	2.520
SUSC	0.420	0.227	1.851	SUSC	0.127	0.090	1.409
Phished Outer Loadings				**Not Phished Outer Loadings**			
	Loading	**SE**	**T Statistics**		**Loading**	**SE**	**T Statistics**
COST	-0.407	0.316	1.288	COST	-0.553	0.105	5.246
EFFECT	0.763	0.319	2.395	EFFECT	0.906	0.048	18.874
RESP	-0.682	0.436	1.564	RESP	-0.652	0.097	6.706
SE	0.648	0.276	2.346	SE	0.495	0.118	4.180
SEV	0.343	0.229	1.497	SEV	0.644	0.100	6.464
SUSC	0.336	0.194	1.736	SUSC	0.142	0.107	1.324

Post-Hoc Analysis

In addition to comprehensive analysis associated with security awareness related to personal threats, the survey participants were also asked to answer the same set of questions related to organizational threats and technical threats. The distinction between the three types was provided to the respondents in the introduction to the survey (see Appendix B for details).

In the previous section, a PLS-MGA approach was implemented to compare the differences between two groups. However, PLS-MGA is designed directly for pairwise comparisons and it can be cumbersome when there are three or more groups to examine. In such situations, it is more useful to employ a multigroup analysis method proposed by Sarstedt, Henseler, and Ringle (2011). This method allows answering the question of whether a parameter differs between the groups. The first step of this approach was used to investigate if the path coefficients are equal across the three groups of threats (i.e., personal, organizational, and technical). The results are included in Table 22. Sample means and standard errors have been obtained from the bootstrapping procedure using 5000 bootstraps and 172 cases.

Table 22

Multigroup Analysis between Personal, Organizational and Technical Information Security Threats

Hypothesis	Path	Personal		Organizational		Technical		F value	p-value
		Sample Mean	SE	Sample Mean	SE	Sample Mean	SE		
H1	EXP -> SA	0.432	0.008	0.436	0.007	0.402	0.009	220.095	0.000
H2	IIS -> SA	0.279	0.007	0.288	0.005	0.276	0.006	35.594	0.000
H3	ISPA -> SA	0.172	0.007	0.168	0.006	0.190	0.005	120.097	0.000
H4	ISPA -> REW	0.167	0.006	0.169	0.006	0.168	0.005	0.670	0.511
H5	ISPA -> SAN	0.332	0.005	0.334	0.005	0.333	0.005	1.273	0.280
H6	SA -> ATT	0.474	0.007	0.501	0.007	0.513	0.006	301.340	0.000
H7	REW -> ATT	0.080	0.004	0.069	0.004	0.070	0.004	50.641	0.000
H8	SAN -> ATT	0.130	0.008	0.117	0.008	0.131	0.007	40.480	0.000
H9	ATT -> INT	0.681	0.005	0.678	0.006	0.676	0.006	6.289	0.002
H10	SA -> INT	0.151	0.006	0.155	0.006	0.155	0.006	3.419	0.033

The results of the multigroup analysis between the three categories of information security threats revealed that there were no significant differences between the three groups for paths between ISPA and REW, as well as between ISPA and SAN; thus providing support for H4 and H5 across the three groups. The multigroup analysis also revealed there were significant differences between the three groups for the remaining paths.

With regards to the relationship between EXP and SA, the employees appear to have most experience with organizational and personal threats, but not with technical threats. In similar fashion, the relationship between IIS and SA is significantly stronger for organizational threats than it is for the other two types. In contrast, the relationship between ISPA and SA is significantly stronger for technical threats. Similarly, the relationship between SA and ATT is significantly stronger for technical threats, followed by organizational threats, and personal threats. The path between REW and ATT is significantly stronger for personal threats than it is for organizational and technical threats. However, the path between SAN and ATT is significantly weaker for organizational threats than it is for personal and technical threats. Nevertheless, the path is not significant across all three models. With regards to the path between ATT and INT, it is significantly stronger for personal threats than it is for the other two groups. Finally, same is true for the path between SA and INT with the exception that it is significantly weaker for personal threats than it is for the other two groups. Still, the path is not significant across all three models.

To further understand the differences across the three groups of threats, the exact same procedure (172 cases and 5000 samples) was applied to analyze the weights of the formative indicators of SA. The results are included in Table 23 and reveal several interesting findings. First, the weight of COST is significantly stronger for personal threats than it is for organizational threats followed by technical threats. Second, the employees' EFFECT is significantly stronger for organizational threats than it is for personal threats, followed by technical threats. Interestingly, the weight for RESP for organizational threats is significantly different from personal and technical threats. Similarly, the weight for SE for organizational threats is significantly smaller than it is for personal and technical threats. Furthermore, the municipality’s employees perceive technical threats as more severe than organizational threats, which in turn are more severe than personal threats. Finally, the survey participants were more susceptible to personal threats than they feel for organizational threats, followed by technical threats.

Table 23

Multigroup Analysis for Personal, Organizational, and Technical Dimensions of SA

	Personal		**Organizational**		**Technical**		**F value**	**p value**
	Sample Mean	**SE**	**Sample Mean**	**SE**	**Sample Mean**	**SE**		
COST	-0.169	0.011	-0.096	0.008	-0.069	0.008	1516.664	0.000
EFFECT	0.549	0.017	0.583	0.017	0.471	0.014	1032.391	0.000
RESP	-0.218	0.010	-0.186	0.010	-0.221	0.011	184.814	0.000
SE	0.206	0.010	0.154	0.011	0.212	0.010	479.698	0.000
SEV	0.231	0.012	0.340	0.008	0.439	0.013	4870.665	0.000
SUSC	0.168	0.008	0.107	0.006	0.056	0.008	2227.551	0.000

CHAPTER 5

DISCUSSION

Discussion of the Findings

This study was divided into two separate observations: (1) the phishing experiment, and (2) the research model questionnaire. A detailed discussion of both instruments is included in the following paragraphs.

The objective of the phishing experiment was to examine whether some of the municipality’s employees are more susceptible to phishing than others. To the best knowledge of the author, this study is one of the first attempts in information systems discipline that examined personal characteristics of individuals susceptible to phishing attacks. Therefore, it is difficult to compare the results with other studies. In addition, the data collection process was administered over a population of only one organization. Consequently, there is a risk the results may not be generalizable towards larger populations. This part of the study was purely exploratory in nature, and driven by the customer’s explicitly stated request. Two types (i.e., regular phishing and spear-phishing) of phishing messages were sent out to the target audience. The regular phishing email yielded 39 unique (76 total) clicks on the fake hyperlink which gives approximately 2.7% response rate. This ratio is in line with the average response rate for this type of scam messages (Hong, 2012; James, 2009). On the other hand, the spear-phishing message yielded 236 unique (338 total) responses that translated to approximately 16.5% response rate. Also, this rate is more than 6 times higher than the one for regular phishing message, which confirms that people are more likely to fall for phishing if they know the sender. In this study, the spear-phishing message mimicked the municipality’s IT support account, and provided the recipients with a contact point to the system administrator. Both messages followed the anatomy of a typical phishing attack, including two out of three critical elements of such attacks; the lure, the hook, but not the catch (Myers, 2007). Per the agreement with the municipality's officials, the author did not collect any personal information from the employees.

The regular phishing message appealed to the individuals' feeling of greed as it offered free coupon for Amazon.com shopping. Usually, most of the people have received similar type of message at some point of their life. Consequently, the vast majority was already familiar with such concepts. On the other hand, the spear-phishing message was crafted specifically for the employees of the municipality, using specific knowledge about the target organization's technology infrastructure and computing policies. In addition, the message was appealing to the employees' sense of urgency, and it warned them about security risks associated with password sharing; thus making the message more convincing. It should be noted that most of organizations can filter unwanted and dangerous email traffic by using email security appliances (e.g., Cisco Email Security Appliance, etc.). Still, some of the unwanted spam and phishing emails are not caught and filtered by the security solutions. Consequently, the members of any organization need to understand how to recognize phishing email, how to report them, and how to avoid such threats.

The customer was also interested in finding out whether there are any common characteristics for individuals who were prone to phishing attacks. This part of the study was purely exploratory in nature. Stepwise discriminant analysis was employed to find the demographic characteristics that best discriminate between those who responded to the phishing emails and those who did not. The analysis revealed there were seven variables that best differentiated between the two groups. First, with regards to factors that increase the probability of being phished, full-time regular employees were found to be more likely to be victimized by phishing scams than individuals employed in other capacity. It is of no surprise because full-time employees constitute the majority of the total employee population in the target organization. In addition, they are using computers and mobile devices connected to the Internet on a regular basis to perform their daily work-related duties. On the other hand, some of the part-time employees do not have their own workstation. In some cases, they share one computer among several individuals employed at similar capacity. The analysis also revealed that individuals between 31 and 35 years old, and individuals with an annual salary between $91k and $100k were more likely to be victimized by the phishing messages. These two groups had very little in common since there was only one employee who was a member of both groups simultaneously. However, every individual from the above salary bracket was a full-time employee. In addition, after consulting with the customer, it was determined that these individuals were primarily employed in managerial positions. Ergo, they spend more time in front of a computer than other employees. Still, future research should address this interesting finding. As of now, it is difficult to propose a more plausible answer as to why this particular salary group was more susceptible to phishing, other than a hypothesis that these individuals are in a position of power and could potentially disregard the prescriptions of the organizational information security policy, as well as the intentions of awareness training activities. Individuals aged between 31 and 35 are the third group in the analysis that was susceptible to phishing. With the exception of three, all of them were full-time regular employees with a slightly higher ratio of men in the group (i.e., 74% vs. 63% in the whole population) with an average annual salary slightly above $46k. They were primarily blue-collar workers (not FLSA exempt). Therefore, it appears that in case of this group, lack of awareness could have been the decisive factor, as opposed to potential ignorance that could be the case for $91-$100k annual salary group. Unfortunately, the customer did not provide the author with additional information about the education levels for the employees, a factor which could possibly shed more light on the findings. Finally, the analysis revealed the employees of a certain business unit are more likely to be victimized by phishing attacks. After consulting with the customer, the IT management group decided to personally investigate the issue in more detail.

At the other end of the spectrum, there are factors that reduce the likelihood of being phished. It was determined that males were less likely to follow phishing messages. With regards to ethnicity, the analysis revealed that Hispanics were less likely to be victimized by phishing attacks in comparison to other ethnic groups. Most of these individuals were full-time employees with an average annual salary of approximately $43k, with vast majority being FLSA non-exempt. Finally, individuals living in a densely populated metropolitan area were found to be less likely to follow the phishing emails' hyperlinks.

After taking into consideration that majority of the victims were tricked by the spear-phishing email, the overall conclusion is that, in general, the customer should take a different approach for relatively well-paid white-collar employees and put more emphasis on the importance of compliance with security policies. On the other hand, in case of younger blue-collar employees it is recommended that more emphasis is placed on the recognition of threats. Nevertheless, even though the results of the discriminant analysis are significant, the findings should be treated with caution because of the relatively low classification accuracy, yet still around the recommended threshold (Hair et al., 2010), of the model.

In the main stage of the study, the research model has been tested using a survey instrument on a sample of 172 employees of the municipality. The participation in the questionnaire was voluntary per the agreement with the customer. First, the whole sample was tested together. The main contribution of the study was to propose and empirically validate the exhaustive and universal contextualization of security awareness as a multidimensional construct. It was proposed that security awareness in organizational settings is a variable composed of six significant components: perceived cost, perceived effectiveness, perceived responsibilities, self-efficacy, perceived severity, and perceived susceptibility. Empirical validation of security awareness as a formative second-order construct provided support for the main proposition of this study. The results show that EFFECT is the strongest component of SA, followed by fairly similar contributions from SE, RESP, SEV, and SUSC. The weight of COST was not significant. Nevertheless, the indicator was retained in the model because its outer loading was significant. The overall results indicate that when it comes to personal information security threats, the study participants primarily rely on their knowledge of how effective the threat countermeasures are. They also take into consideration whether they are able to exercise the recommended protective actions, and include the evaluation of risks associated with personal threats (i.e., how likely a threat is to occur combined with the magnitude of the consequences if affected by such threat). Finally, the municipality’s employees also consider their respective responsibilities with regards to the occurrence of a threat. Therefore, the results provide support for the claim that individuals understand the relationship between personal threats and potential negative outcomes for their organization. Consequently, RESP has been shown as a significant element of building SA. Somewhat unexpectedly, COST did not significantly contribute to SA. One possible explanation is that personal security threats are directly aimed at a given person. As a result, they will attempt to learn how to avoid such direct threat, regardless of the cost that the action would involve. On the other hand, COST was operationalized primarily as an element of inconvenience and overhead. A more complete picture could potentially be obtained if the cost of avoiding threats was contextualized in terms of financial, cognitive, and time efforts. In organizational settings the financial element of the construct is not present since the employees are usually provided with proper means that should assist them in avoiding threats. Thus, the second explanation for COST's lack of significance is that the customer does its diligence and makes sure that employees have proper tools at hand that do not inconvenience their daily routines.

The next goal of the study was to determine what the antecedents of security awareness are. Following the prescriptions of PMT (Floyd, Prentice-Dunn, & Rogers, 2000; Milne et al., 2000), two main categories of antecedents were identified: environmental and intrapersonal. The former can involve communication and observational learning. It was operationalized through ISPA and IIS. The latter can involve personality-related traits and prior experience (operationalized through EXP). Personality scales were not implemented to avoid potential respondent fatigue, as related scales tend to be long. All three constructs were found to be significant and positive predictors of SA. Consequently, data analysis provides support for H1, H2, and H3. The three constructs collectively explain 53.3% of variance in SA. EXP turned out to be strongest its predictor with a medium effect size, while IIS and ISPA had a small effect size. These results are logical, as knowledge of security policy does not inform the individuals about the full spectrum of awareness components. Security policies are usually high-level documents that outline the basics of areas like computer and network usage, email policies, authentication, mobile technology usage, web browsing rules, etc. (Boyle & Panko, 2013; West, 2009). Thus, the members of the organization most likely learn about the costs and responsibilities from security policies. They may also acquire basic knowledge of risks, but not necessarily knowledge and understanding of prescriptive actions. Similarly, not all individuals are expected to be interested in learning about information security threats on their own. Thus, it is not suspiring that both ISPA and IIS have a small effect size on SA. Still, both predictors were significant. This is an important finding from the perspective of the target organization. It means the municipality has achieved some level of success in effectively communicating the importance of information security. It also means that, at least to some extent, the members of the organization are interested in learning about security threats on their own. Consequently, the effectiveness of information security training and reinforcement programs should be high, since the organization appears to have established a security culture among its employees. Nevertheless most of SA is gained through previous experience with threats. This means that direct exposure and experiencing threats “the hard way” remain the most effective methods of learning for most individuals. While at first this finding may sound a bit discouraging for the customer’s IT management, it actually provides the customer with an excellent opportunity to increase the effectiveness of training activities. The customer should considering creating a more interactive training approach by designing awareness building activities that would include simulated behaviors and effects of information security threats. For example, as it was done in this study, customer could design a set of phishing messages that would be sent to the employees. As a follow-up, the IT management could then notify the employees about the threat, explain the negative consequences, and educate the employees about how to recognize phishing emails and how to avoid them in the future. To the best knowledge of the author, most of the organizations limit their security training activities to a passive transmission of information that requires little to no cognitive involvement from the training recipients. While, the more interactive approach could be more expensive to implement, organizations should still consider it seriously, as it may result in future cost savings through lower exposure to threats.

The study's results also provide support for hypotheses H4 and H5. That is, awareness of security policy (ISPA) is a significant predictor of rewards (REW) and sanctions (SAN). This important finding provides further support for the claim that the customer is able to effectively communicate the prescriptions included in the information security policy to its employees. In previous studies (Bulgurcu et al., 2010) REW and SAN were conceptualized as consequences of general security awareness. However, this study separates awareness of threats with awareness of security policy. While the latter can serve as one of the antecedents of the former (vide support for H3), it is impossible to expect that knowledge about REW and SAN would be a consequence of SA.

The next step of the analysis was to determine the impact of REW and SAN on attitude towards compliance with information security policy (ATT). The results did not provide support for any significant effect of rewards or sanctions on attitude (i.e., lack of support for H7 and

H8). Both of these constructs have strong roots in GDT. As previously noted, studies implementing elements of deterrence are inconclusive with regards to the impact of sanctions and punishment on compliance. The present study's results add an important piece to the current body of knowledge in this area. Per the discussion with the customer, it has been established that the target organization does not punish non-compliant behaviors with any sanctions; nor does it actively reward compliance. Ergo lack of significant relationship between SAN and ATT, as well as REW and ATT. Per the discussion of previous research (Ball et al., 2010; Straub & Welke, 1998), certainty of sanctions could shed more light on this interesting topic. Still, the inclusion of the above in the present study, most likely, would not affect the results as the municipality does not enforce any type of consequences for being in line with requirements specified in the security policy.

With the lack of support for H7 and H8, SA is the only significant predictor of ATT (support for H6) that explains approximately 27% of variance in the attitude towards compliance. While initially this number may appear to be small or moderate, in fact it should be considered fairly high in light of previous studies. For example, Bulgurcu et al. (2010) report 26% of variance explained in attitude by 4 significant predictors including their conceptualization of awareness and other variables pertaining to beliefs about consequences. Other studies on attitude towards compliance identify different antecedents of the construct that explain the variance in it to a varying degree (Guo, Yuan, Archer, & Connelly, 2011; Herath & Rao, 2009b; Pahnila et al., 2007). These studies identify different sources of ATT. Consequently, future research should address their effect size once all included in a research model. More interestingly, however, the present study's results reveal that ATT fully mediates the relationship between SA and INT (i.e., through support for H6 and H9, but not H10). This finding is important from both theoretical and practical perspectives. It shows that the path to compliance leads through attitudes, as ATT is a strong and significant predictor of INT in this study and across other aforementioned studies as well.

Additionally, the design of the study allowed for separation of the direct observation of behavior from the self-reported survey instrument. Falling victim to the phishing email is essentially an example of a non-compliant behavior. Furthermore, phishing is an example of personal information security threats. Therefore, it was justified to split the participants into two separate groups; those who got victimized by any of the phishing messages and those who did not. PLS-MGA results reveal some interesting insights. First, the phished group appears lack security awareness. None of SA's components was significantly contributing to the second-order construct. Only SUSC was marginally significant at p = 0.1. This means that phished individuals only respond to threats if they perceive the likelihood of being affected by the threat to be high. However, they do not understand the consequences of being affected by it, nor do they possess proper set of avoidance skills. Finally, they also did not know what they responsibilities were with regards to threat avoidance. Thus, it appears their awareness was limited to relying more on instincts than any other quantifiable source of information. On the other hand, the "not phished" group relied primarily on two measures: EFFECT and SEV. Thus, these individuals already demonstrated some level of objective knowledge of threats and their respective countermeasures. Still, they were not able to measure the likelihood of being affected by a threat (i.e., non-significant weight of SUSC), and they were not sure about their capabilities to implement the recommended protective behaviors (i.e., non-significant weight of SE). In case of both groups the weights of COST and RESP were not significant. While it is clear that both groups are different and that non-phished group demonstrated evidence of some levels of rational knowledge about threat avoidance, the overall results should be treated with care; the values of the measurement errors as described in Table 18 are relatively high, especially for the phished group. This is most likely because of the relatively small sample size. The true values could be slightly higher. Still, the differences between the two groups are clearly visible and can be explained from a theoretical perspective.

Further support for the evident differences between the groups is found in comparison of the research model's hypotheses. First of all, in case of the phished group H1 through H3 were not supported. Since none of the antecedents of awareness was significant, it is of no surprise that the individuals did not have SA, so to say. On the other hand, the not-phished group exhibited some levels of prior experience and interest in information security (i.e., support for H1 and H2), but indicated some deficiencies in knowing the prescriptions of the information security policy (i.e., H3 not supported). Hence, the non-significant weights of RESP and COST are justified. It appears that high levels of EXP and IIS primarily impact EFFECT and SUSC, but not the other components of SA. Therefore, the customer should consider emphasizing SEV and SE in their future security training efforts. As mentioned, the overall results for both groups may be slightly deflated due to the presence of relatively high measurement error levels, most likely caused by the small sample size.

It appears that both groups were able to derive proper knowledge of sanctions for non-compliance (i.e., support for H5). On the other hand, not-phished group did not see any personal rewards that could be obtained from demonstrating compliant behaviors (i.e., lack of support for H4). It was also of no surprise that H6 was not supported for the phishing victims. Simply put, if these individuals do not have security awareness, it would be impossible to expect that SA would have any significant impact on ATT. From a compliance perspective, these individuals should be given additional attention when designing security training activities, because initially they will not have proper foundations allowing them to understand the importance of information security issues, and consequently, affect their attitude towards compliance with security policies. The study results show that attitude is the single most important factor determining intention to comply.

Finally, the post-hoc analysis was conducted to analyze if there were any differences in dimensions of awareness across three different types of security threats: personal (the main focus of the study), organizational, and technical. The comparison of the three categories of threats is presented in Table 20. COST has been determined to be most strongly associated with personal threats, followed by organizational and technical threats. It is of no surprise, because personal threats are the most palpable for individuals. On the other hand, it is also possible that individuals perceive that the cost of avoiding organizational and technical threats should be shifted towards the employer, while avoiding personal threats is strictly tied to an individual. In addition, the cost of avoiding technical threats often requires little to no interventions from individuals. For example, antimalware software can automatically scan computers and remove threats as they are discovered. At the end of the process, the user may or may not be presented with the summary of the analysis. Therefore, avoiding technical threats is not really a burden in the organizational settings. This finding is also supported by the lower levels of SUSC for technical threats in comparison with organizational and personal threats. In contrast, it can be reversed in home settings where the users need to take care of security on their own.

The participants also felt that they most effectively could avoid organizational threats. The most plausible explanation is that organizational threats require relatively less technical expertise. Moreover, some organizational threats (e.g., data handling procedures, information disclosure, ignoring information security policy) are often outlined in the information security policy. Since every employee was subjected to initial information security policy training upon hiring, it was easy for the individuals to verify what type of behaviors would lead to expected outcomes. This finding is also backed by the support for H4 and H5. On the other hand, the study participants demonstrate significantly lower levels of self-efficacy with avoiding organizational threats in comparison with the remaining two threat categories. It is possible that while they are properly educated on the types of avoidance behaviors expected of them (expressed through higher levels of EFFECT), they may lack hands-on experience with avoiding certain threats. Another, less plausible explanation is that the municipality's employees have not been exposed to any organizational threats, but they have been exposed to some degree of personal and technical threats. A third alternative is that they do not perceive avoidance of organizational threats to be their responsibility, which is expressed through a significantly lower levels of RESP for organizational threats than it is the case for personal and technical threats. It is also possible that the negative effects of organizational threats are not directly observable by the employees, which could mean they do not feel personally responsible for avoiding them. The above would explain why the participants perceived technical threats to be more severe than organizational threats. On the other hand, the participants felt that personal threats were the least severe of the three categories. It could be so, because they felt most familiar about personal threats. More likely however, as the results of the main study indicate, it was because the individuals' previous experience with threats is primarily related to the effectiveness of the countermeasures and the likelihood of being affected by threats. The latter explanation is supported by the fact that the employees felt more susceptible to personal threats than they did for the remaining two categories of threats.

Overall, the municipality should direct more attention towards informing the employees about every dimension of security awareness. The customer should also emphasize that while some of the protections against threats are or can be fully automated, the employees should still be held responsible for being aware of how different threats should be handled. After all, it is one of the principles in modern information systems design to have a built-in redundancy solution in case of the system's failure. As it is in case of phishing, most of the scam is usually filtered out by the email-filtering systems; some of the unwanted messages still manage to reach the targeted recipients. Ultimately, the overall security of the system is dependent upon the human factor.

Theoretical Contributions

This study had addressed four major research gaps. First, it proposed and empirically validated a multidimensional (Dinev & Hu, 2007) definition of security awareness based on combination of the well-known theoretical foundations of TTAT and PMT, and combining them with the elements of GDT, TRA, and TPB. Security awareness has been defined as a second-order formative construct composed of perceived susceptibility, perceived severity, self-efficacy, perceived effectiveness, perceived costs, and a new construct – responsibilities. To best knowledge of the author it is also one of the first studies to have successfully implemented a higher-order construct on the elements of PMT (Floyd et al., 2000; Milne et al., 2000). As a result, a universal yet exhaustive definition of security awareness is now available to other scholars. Future studies in the topic will now be able to compare their results across different settings. Additionally, it will also be possible to discuss the issues and the effects on the nomological network across different studies (Gefen, Rigdon, & Straub, 2011). Moreover, the proposed definition of awareness builds upon previous studies in the area and matches with practitioner approaches. As a result, the current body of knowledge does remain significant part of this research stream. The proposed definition also bridges the gap between academic and practitioner worlds, increasing the practical relevance of the scholarly work, while maintaining strict academic rigor in the study's execution. Finally, the proposed definition of awareness defines it as a state knowledge rather than a process. This state of knowledge accounts for the temporal aspect (Sarter & Woods, 1991) of awareness that differentiates it from full knowledge of the topic. It also makes the approach applicable to information security area, because threat avoidance often requires quick decisions based upon limited resources available to the subject.

This study has also examined the antecedents of security awareness, an important research gap identified by previous literature (Bulgurcu et al., 2010). These have been theoretically identified through the assumptions of PMT, and conceptualized through previous experience with security threats, interest in security threats, and awareness of information security policy. All three constructs were significant predictors of security awareness. This design also accounted for information acquired from the surrounding environment (i.e., security policy awareness, and interest in security threats) as well as intrapersonal factors contextualized through prior experience.

This study has also examined whether security awareness is a significant factor determining compliance with information security policies. The results provide support for the above relationship, with the exception that it was fully mediated by the attitude towards compliance. It appears that awareness is one of many factors affecting people's attitudes. Future research should examine what the other predictors are.

Finally, the present study has also addressed a common issue of delineating between behavioral intentions and exercising actual behavior. This has been accomplished through direct observation of non-compliant behaviors, and conducting the PLS-MGA analysis. The results reveal that while attitude remained a significant predictor of behavioral intention, the individuals who maintain compliance with security policies were significantly different from their non-compliant counterparts in terms of the levels of security awareness.

Practical Implications

While the study was executed following the requirements of rigorous research, it also does offer substantial insights for the practitioner realm. With regards to the practitioner perspective, this study had two main objectives. First, it proposed and developed a comprehensive instrument that allows for a quick assessment of security awareness among the individuals employed by an organization. Second, the study's instrument was also designed to facilitate building effective and comprehensive security awareness and training programs. The survey instrument examined six dimensions of security awareness. Furthermore, it was designed to account for different type of threats. Consequently, organizations can adjust the instrument in order to obtain a customized focus and granularity levels. Most importantly, the instrument allows for a quick identification of potential weaknesses in information security awareness, and thus, it will facilitate the design of either a quick reinforcement activity or a training program that addresses such deficiencies. The study's results reveal that the survey instrument is capable of capturing the differences between individuals who remained in compliance with security policies and those who did not. The present research operationalized the security awareness model to test for differences in how individuals responded to phishing. The instrument was proven to be a robust tool allowing for the identification of significant differences between the two groups. Furthermore, the instrument was designed in such a way so it would work for other scenarios as well. Therefore, it is a powerful tool backed by strong theoretical foundations that can be employed in a plethora of settings; for example, across different organizations, or across different business units within one organization.

Limitations and Future Research

As it is the case with majority of other studies, the present research is subject to several limitations. First, the generalizability of the results can be questionable. Both the phishing experiment and they survey instrument were administered to the employees of a single organizations, a municipality in north Texas. Consequently, the findings of this study are representative of this particular organization only and may not be true of other organizations in the state or the country.

Second, the data in this study were collected in a cross-sectional manner. Consequently, the causality between the variable may be questionable, even though the hypotheses proposed in this study are based on solid theoretical background. If so, it is possible that, at best, the data supports the existence of correlation between the constructs rather than unidirectional relationships. For example, at the initial stages, SA leads to the development of attitudes towards compliance. However, once individuals develop positive attitudes towards compliance, they may also put more emphasis on increasing their levels of awareness (e.g., through an increased interest in information security topics, including security threats). This limitation can be addressed through conducting a longitudinal study to examine the true nature of the hypothesized relationships.

Third, another potential limitation is related to the outer loadings of ATT and INT. In both situations, the loadings are above the recommended maximum threshold of 0.95. The measurement scales for these items were adapted from previously validated studies (Ajzen, 1991; Bulgurcu et al., 2010), the results of which did not indicated any potential issues with the measurement items. The pilot study conducted by the author did not reveal any problems at this level as well.

Fourth, another potential limitation can be related to the operationalization of COST. In this study the cost of avoiding information security threats was contextualized as a burden preventing the participants from performing their everyday duties in the workplace. However, a more detailed decomposition of the variable could reveal further insights into the nature of the construct. For example, COST could be operationalized in terms of three dimensions: cognitive, temporal, and financial. As previously mentioned, the design of the questionnaire was a compromise between addressing the issue of respondent fatigue per the requirements expressed by the customer and maintaining sufficient level of depth.

For the same reasons, the conceptualization of the elements of deterrence (i.e., REW and SAN) could potentially be somewhat simplified as well. While the results reveal that the municipality's human resources unit does its due diligence in making sure that new hires are aware of rewards and sanctions included in the information security policy, the customer's IT management does not actively pursue enforcing these regulations. It is possible that inclusion of additional variable could shed more light on the phenomenon of attitude development. For example, certainty and swiftness (Ball et al., 2010) of sanctions could explain why deterrence elements does not significantly affect the attitude towards compliance with the information security policy.

Future research directions should basically attempt to address the above limitations. First of all, the instrument should be tested across other populations. This study has been executed over the population of municipal employees in one organization only. It is desirable to cross-examine the results with other organizations, both in public and private sectors. More importantly, future research should take a longitudinal approach and examine the effects of security awareness and training programs on the development of employees' awareness, attitudes, and compliance. Consequently, it would be possible to estimate the key drivers in human behavior that would maximize compliance with information security policies, and help build security-oriented culture in organizations.

Conclusions

The present study proposed and validated a unified multidimensional and exhaustive definition of security awareness that allows for standardized comparisons of results across different populations and different settings. It bridges the gap between theory and practice.

The proposed definition draws heavily on both fields, thus maintaining proper academic rigor and delivering results that could be applied in practice. As a result, the results of the study make significant contribution in both areas. This study has also examined the antecedents of security awareness of security awareness, a gap that has not been previously addressed by academics. The proposed research model and instrument offer a solution readily available to be implemented in organizations. This study also makes an important contribution in that it examines actual human behavior (operationalized through responses to the phishing experiment) rather than behavioral intentions only.

APPENDIX A

SURVEY INSTRUMENT

University of North Texas Institutional Review Board

Informed Consent Notice

Before agreeing to participate in this research study, it is important that you read and understand the following explanation of the purpose, benefits and risks of the study and how it will be conducted.

Title of Study: The impact of information security awareness on compliance with information security policies. A phishing perspective.

Investigator: Dr. John Windsor, University of North Texas (UNT) Department of Information Technology and Decision Sciences ITDS Dept.). Student Investigator: Bartlomiej Hanus, ITDS Dept.

Purpose of the Study: You are being asked to participate in a research study which involves an investigation of your perceived levels of information security awareness, and helps design information security awareness training. This study is being administered by University of North Texas for the [redacted].

Study Procedures: You will be asked to complete a questionnaire regarding your perceived levels of information security knowledge and awareness that will take 20-30 minutes of your time. The questionnaire is anonymous, and no information that could identify you personally will be collected.

Foreseeable Risks: No foreseeable risks are involved in this study.

Benefits to the Subjects or Others: We expect the project to benefit you by allowing us to design an effective information security awareness training program that may help you identify potential information security threats at your workplace and home environments that can impact your personal and professional experience. The results of the study may also allow us to determine the areas of information security awareness that should be improved through training. The results of the study may also be beneficial to our community by raising overall security awareness of its members.

Compensation for Participants: None.

Procedures for Maintaining Confidentiality of Research Records: The questionnaire is fully anonymous and no personal information will be collected during the procedure. The confidentiality of your individual information will be maintained in any publications or presentations regarding this study.

Questions about the Study: If you have any questions about the study, you may contact Bartlomiej Hanus at bartlomiej.hanus@unt.edu or Dr. John Windsor at john.windsor@unt.edu.

Review for the Protection of Participants: This research study has been reviewed and approved by the UNT Institutional Review Board (IRB). The UNT IRB can be contacted at (940) 565-3940 with any questions regarding the rights of research subjects.

Research Participants' Rights: Your participation in the survey confirms that you have read all of the above and that you agree to all of the following:

- Dr. John Windsor has explained the study to you and you have had an opportunity to contact him/her with any questions about the study. You have been informed of the possible benefits and the potential risks of the study.
- You understand that you do not have to take part in this study, and your refusal to participate or your decision to withdraw will involve no penalty or loss of rights or benefits. The study personnel may choose to stop your participation at any time.
- You understand why the study is being conducted and how it will be performed.
- You understand your rights as a research participant and you voluntarily consent to participate in this study.
- You understand you may print a copy of this form for your records.

INFO

This questionnaire investigates your levels of information security awareness by assessing your perceptions about information security threats. Within the area of information security, a threat is defined as a potential cause of an incident that may result in harm to a person, a system, or an organization. In other words, a threat is an event that may defeat the security measures in place and result in a loss.

For the purpose of this survey, information security threats are classified into three categories:

- Organizational threats that refer to:

    - ignoring sensitive data handling procedures (e.g., dumspter diving, discarded media, etc.),
    - ignoring information security policy,
    - compromises to intellectual property (piracy, copyright infringement),
    - information disclosure,
    - unauthorized physical access to buildings and equipment,.
- Personal (human factor) threats which refer to:
    - managing passwords,
    - leaving computer unattended while logged in,
    - social engineering (misinterpretation, impersonation),
    - phishing and spam,
    - abuse of trust in social networks,
    - human errors.
- Technology threats, referring to:
    - malicious code (malware) like viruses, worms, Trojan horses,
    - unknown email attachments,
    - communication interception (e.g., wiretapping, eavesdropping)
    - breaching access controls (brute force attacks, wardriving, etc.)
    - hardware and software failures,
    - mobile threats (unwanted software, spyware, malware, etc.).

The survey often refers to the above three categories of threats. When responding to questions, please have in mind what these categories include.

The survey is anonymous, so responses will not be tied to any individuals. Your participation will allow us to create effective information security training program that will be beneficial to our community. Thank you for your participation!

REW ____ I comply with the requirements of the Information Security Policy.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
I will receive personal mention in oral or written assessment reports if (1)	❍	❍	❍	❍	❍	❍	❍
I will be given monetary or non-monetary rewards if (2)	❍	❍	❍	❍	❍	❍	❍
My receiving tangible or intangible rewards are tied to whether (3)	❍	❍	❍	❍	❍	❍	❍

SAN ____ I don't comply with the requirements of the Information Security Policy.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
I will probably be punished or demoted if (1)	❍	❍	❍	❍	❍	❍	❍
I will receive personal reprimand in oral or written assessment reports if (2)	❍	❍	❍	❍	❍	❍	❍
My facing tangible or intangible sanctions is tied to whether (3)	❍	❍	❍	❍	❍	❍	❍

EXP1 I have the necessary skills and knowledge about security threats related to ____.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

EXP2 How confident are you in your ability to deal with information security threats related to:

	1 - Not at all confident	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely confident
Organizational factors (1)	○	○	○	○	○	○	○
Personal factors (2)	○	○	○	○	○	○	○
Technological factors (3)	○	○	○	○	○	○	○

EXP3 My knowledge of security threats related to ____ is:

	1 - Low	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - High
Organizational factors (1)	○	○	○	○	○	○	○
Personal factors (2)	○	○	○	○	○	○	○
Technological factors (3)	○	○	○	○	○	○	○

IIS Please indicate your level of agreement with the following statements:

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Assuming I have access to information security related materials, I intend to learn more about information security threats. (1)	○	○	○	○	○	○	○
I plan to learn more about information security threats, so that I can avoid them. (2)	○	○	○	○	○	○	○
Given that I have access to learning materials, I predict I would learn more about information security threats and countermeasures. (3)	○	○	○	○	○	○	○
I learn how information security threats can be part of my everyday life. (4)	○	○	○	○	○	○	○
I think that information security is an important issue. (5)	○	○	○	○	○	○	○

ISPA Please indicate your level of agreement with the following statements:

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
I am aware of my organization's information security policy (1)	○	○	○	○	○	○	○
I know the rules and regulations prescribed by the information security policy of my organization. (2)	○	○	○	○	○	○	○
I understand the rules and regulations prescribed by the information security policy of my organization. (3)	○	○	○	○	○	○	○
I know my responsibilities as prescribed in the information security policy to enhance the IS security of my organization. (4)	○	○	○	○	○	○	○

SUSC1 The chances of me being affected by security threats related to ____ are high.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SUSC2 Taking all possible factors into consideration, what do you think is the risk of you being affected by information security threats related to:

	1 - Extremely low (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely high (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SUSC3 Taking all possible factors into consideration, do you think it is possible that you can be exposed to information security threats associated with:

	1 - Not possible at all (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely possible (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SUSC4 Taking all possible factors into consideration, I am likely to be exposed to information security threats related to:

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SEV1 On a scale from 1 to 7, in your opinion how serious do you think are information security threats associated with:

	1 - Not serious at all (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely serious (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SEV3 On a scale from 1 to 7, in your opinion how significant do you think are information security threats associated with:

	1 - Not significant at all (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely significant (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SEV2 On a scale from 1 to 7, in your opinion how severe do you think are information security threats associated with:

	1 - Not severe at all (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely severe (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SEV4 I believe the productivity of my organization and its employees could be threatened by security threats related to:

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

EFFECT1 In your opinion, how effective do you think you are in avoiding information security threats associated with:

	1 - Not effective at all (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely effective (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

EFFECT2 In your opinion, how confident do you think you are in avoiding information security threats associated with:

	1 - Not at all confident (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Extremely confident (7)
Organizational factors (1)	○	○	○	○	○	○	○
Personal factors (2)	○	○	○	○	○	○	○
Technological factors (3)	○	○	○	○	○	○	○

EFFECT3 I can make a difference in helping to secure my organization from security threats related to:

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	○	○	○	○	○	○	○
Personal factors (2)	○	○	○	○	○	○	○
Technological factors (3)	○	○	○	○	○	○	○

SE1 I could avoid information security threats related to ____ if there was no one around to tell me what to do.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	○	○	○	○	○	○	○
Personal factors (2)	○	○	○	○	○	○	○
Technological factors (3)	○	○	○	○	○	○	○

SE2 I am confident that I could avoid information security threats related to ____ if I had never seen them before.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SE3 I would feel comfortable with avoiding most of the security threats related to:

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

SE4 If I wanted to, I could easily avoid security threats related to ____ on my own.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

COST1 Avoiding information security threats related to ____ inconveniences my work.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

COST2 There is too much overhead associated with avoiding information security threats related to:

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

RESP1 With regards to security threats related to ____, protection of organizational information is not my problem.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

RESP2 With regards security threats associated with ____, reporting information security threats is none of my concern.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

RESP3 If I discovered a security threat related to ____, I would have no idea what my responsibilities are with regards to dealing with such threat.

	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Agree nor Disagree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
Organizational factors (1)	❍	❍	❍	❍	❍	❍	❍
Personal factors (2)	❍	❍	❍	❍	❍	❍	❍
Technological factors (3)	❍	❍	❍	❍	❍	❍	❍

ATT To me, complying with the requirements of the information security policy is:

	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (7)
Unnecessary:Necessary (1)	❍	❍	❍	❍	❍	❍	❍
Unbeneficial:Beneficial (2)	❍	❍	❍	❍	❍	❍	❍
Unimportant:Important (3)	❍	❍	❍	❍	❍	❍	❍
Useless:Useful (4)	❍	❍	❍	❍	❍	❍	❍

INT Please indicate your level of agreement with the following statements:

	1 - Strongly disagree (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 - Strongly agree (7)
I intend to comply with the requirements of the information security policy of my organization in the future. (1)	❍	❍	❍	❍	❍	❍	❍
I intend to protect information and technology resources according to the requirements of the information security policy of my organization in the future. (2)	❍	❍	❍	❍	❍	❍	❍
I intend to carry out my responsibilities prescribed in the information security policy of my organization when I use information and technology in the future. (3)	❍	❍	❍	❍	❍	❍	❍

APPENDIX B

INDEPENDENT SAMPLES TEST

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Gender_Male	A	10.237	.001	1.895	1634	.058	.067	.035	-.002	.136
	B			1.835	262.141	.068	.067	.036	-.005	.138
E_White	A	38.587	.000	-2.789	1634	.005	-.084	.030	-.142	-.025
	B			-3.222	299.379	.001	-.084	.026	-.135	-.033
E_Black	A	1.571	.210	.620	1634	.535	.012	.019	-.025	.049
	B			.660	279.503	.510	.012	.018	-.023	.047
E_Hispanic	A	30.560	.000	2.591	1634	.010	.061	.023	.015	.107
	B			3.284	329.145	.001	.061	.018	.024	.097
E_AmericanIndian_AlaskanNative	A	1.251	.264	-.560	1634	.575	-.003	.006	-.015	.009
	B			-.477	244.739	.634	-.003	.007	-.018	.011
E_Asian_or_Pacific_Islander	A	3.314	.069	.904	1634	.366	.007	.008	-.008	.022
	B			1.248	366.569	.213	.007	.006	-.004	.018
E_Two_or_More_Races	A	1.737	.188	.658	1634	.511	.002	.003	-.004	.008
	B			1.733	1429.000	.083	.002	.001	.000	.004
age_by_5_less_eq_20	A	31.329	.000	2.689	1634	.007	.039	.014	.010	.067
	B			5.309	838.514	.000	.039	.007	.024	.053
age_by_5_21_and_25	A	5.769	.016	1.173	1634	.241	.024	.021	-.016	.065
	B			1.310	290.476	.191	.024	.019	-.012	.061
age_by_5_26_and_30	A	3.950	.047	.974	1634	.330	.021	.021	-.021	.063
	B			1.060	284.334	.290	.021	.020	-.018	.060
age_by_5_31_and_35	A	3.597	.058	.928	1634	.354	.022	.023	-.024	.068
	B			.994	280.879	.321	.022	.022	-.021	.065
age_by_5_36_and_40	A	.055	.815	-.117	1634	.907	-.003	.026	-.053	.047
	B			-.116	266.071	.908	-.003	.026	-.054	.048
age_by_5_41_and_45	A	1.767	.184	.653	1634	.514	.017	.026	-.034	.069
	B			.677	274.403	.499	.017	.025	-.033	.067
age_by_5_46_and_50	A	2.240	.135	-.763	1634	.446	-.019	.025	-.068	.030
	B			-.729	259.985	.467	-.019	.026	-.071	.032
age_by_5_51_and_55	A	3.272	.071	-.921	1634	.357	-.020	.022	-.063	.023
	B			-.861	256.784	.390	-.020	.023	-.066	.026
age_by_5_56_and_60	A	14.789	.000	-1.992	1634	.047	-.042	.021	-.084	-.001
	B			-1.739	247.694	.083	-.042	.024	-.090	.006
age_by_5_61_and_65	A	4.011	.045	-1.013	1634	.311	-.016	.015	-.046	.015

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
	B			-.906	250.712	.366	-.016	.017	-.049	.018
age_by_5_over_65	A	11.020	.001	-1.685	1634	.092	-.023	.013	-.049	.004
	B			-1.384	240.923	.168	-.023	.016	-.055	.010
Married	A	1.394	.238	-.742	1634	.458	-.028	.037	-.100	.045
	B			-.739	266.627	.461	-.028	.037	-.101	.046
work_exp_by_5_5_or_less	A	8.025	.005	1.268	1634	.205	.045	.036	-.025	.116
	B			1.296	271.541	.196	.045	.035	-.024	.114
work_exp_by_5_6_and_10	A	.154	.695	.194	1634	.846	.006	.031	-.054	.066
	B			.196	268.608	.845	.006	.030	-.054	.066
work_exp_by_5_11_and_15	A	3.092	.079	-.909	1634	.364	-.027	.030	-.085	.031
	B			-.875	261.201	.382	-.027	.031	-.087	.034
work_exp_by_5_16_and_20	A	.240	.624	-.246	1634	.806	-.005	.022	-.049	.038
	B			-.241	264.136	.809	-.005	.023	-.050	.039
work_exp_by_5_21_and_25	A	12.714	.000	-1.831	1634	.067	-.034	.019	-.071	.002
	B			-1.577	246.151	.116	-.034	.022	-.077	.009
work_exp_by_5_26_and_30	A	18.959	.000	2.111	1634	.035	.032	.015	.002	.061
	B			3.146	413.639	.002	.032	.010	.012	.051
work_exp_by_5_31_plus	A	8.006	.005	-1.430	1634	.153	-.016	.012	-.039	.006
	B			-1.171	240.677	.243	-.016	.014	-.044	.011
annual_by_10k_less_eq_20	A	32.037	.000	2.669	1634	.008	.056	.021	.015	.098
	B			3.615	357.425	.000	.056	.016	.026	.087
annual_by_10k_21_and_30	A	1.097	.295	.518	1634	.604	.011	.022	-.031	.054
	B			.540	275.259	.590	.011	.021	-.030	.052
annual_by_10k_31_and_40	A	.243	.622	-.249	1634	.804	-.007	.030	-.066	.051
	B			-.246	265.464	.806	-.007	.030	-.067	.052
annual_by_10k_41_and_50	A	3.860	.050	.949	1634	.343	.028	.030	-.030	.086
	B			.991	275.513	.323	.028	.028	-.028	.084
annual_by_10k_51_and_60	A	3.611	.058	-.973	1634	.331	-.024	.025	-.072	.024
	B			-.917	258.072	.360	-.024	.026	-.075	.027
annual_by_10k_61_and_70	A	2.111	.146	.713	1634	.476	.018	.025	-.031	.066
	B			.747	276.182	.456	.018	.024	-.029	.064
annual_by_10k_71_and_80	A	.604	.437	.386	1634	.699	.008	.020	-.031	.046
	B			.400	273.976	.690	.008	.019	-.030	.045

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
annual_by_10k_81_and_90	A	11.379	.001	-1.717	1634	.086	-.025	.015	-.054	.004
	B			-1.431	242.471	.154	-.025	.018	-.060	.010
annual_by_10k_91_and_100	A	13.391	.000	-1.851	1634	.064	-.020	.011	-.041	.001
	B			-1.429	235.058	.154	-.020	.014	-.047	.008
annual_by_10k_101_plus	A	35.042	.000	-3.033	1634	.002	-.042	.014	-.069	-.015
	B			-2.247	231.671	.026	-.042	.019	-.079	-.005
GENERALFUNDBS	A	19.653	.000	1.564	1634	.118	.058	.037	-.015	.131
	B			1.569	268.149	.118	.058	.037	-.015	.131
SOLIDWASTEBS	A	3.181	.075	-.905	1634	.366	-.017	.019	-.055	.020
	B			-.837	255.277	.403	-.017	.021	-.058	.024
WASTEWATERBS	A	9.355	.002	-1.566	1634	.117	-.030	.019	-.067	.008
	B			-1.380	248.798	.169	-.030	.022	-.073	.013
TECHNOLOGYSERVICESBS	A	27.895	.000	-2.681	1634	.007	-.030	.011	-.051	-.008
	B			-1.922	229.160	.056	-.030	.015	-.060	.001
RECREATIONFUNDBS	A	44.746	.000	3.180	1634	.001	.047	.015	.018	.076
	B			8.381	1429.000	.000	.047	.006	.036	.058
WATERFUNDBS	A	.123	.726	-.176	1634	.860	-.004	.023	-.049	.041
	B			-.174	265.081	.862	-.004	.023	-.049	.041
ELECTRICFUNDBS	A	7.014	.008	-1.359	1634	.174	-.030	.022	-.073	.013
	B			-1.237	253.016	.217	-.030	.024	-.077	.018
AQUATICCENTERFUNDBS	A	7.185	.007	1.313	1634	.189	.022	.017	-.011	.055
	B			1.564	308.198	.119	.022	.014	-.006	.050
STREETIMPROVEMENTFUNDBS	A	.027	.869	.082	1634	.934	.001	.010	-.020	.021
	B			.083	270.101	.934	.001	.010	-.019	.021
FLEETBS	A	10.379	.001	-1.625	1634	.104	-.015	.009	-.033	.003
	B			-1.246	234.522	.214	-.015	.012	-.039	.009
AIRPORTBS	A	4.686	.031	-1.084	1634	.279	-.003	.003	-.010	.003
	B			-.698	222.303	.486	-.003	.005	-.013	.006
RISKRETENTIONBS	A	.362	.547	-.301	1634	.763	-.001	.005	-.010	.007
	B			-.266	249.235	.790	-.001	.005	-.011	.009
MATERIALSMANAGEMENTBS	A	.800	.371	.446	1634	.656	.003	.006	-.010	.015

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
	B			.528	306.213	.598	.003	.005	-.008	.013
Fulltimeregular	A	24.552	.000	-2.307	1634	.021	-.062	.027	-.115	-.009
	B			-2.678	300.725	.008	-.062	.023	-.108	-.017
Parttimeregular	A	39.922	.000	2.911	1634	.004	.073	.025	.024	.123
	B			3.693	329.543	.000	.073	.020	.034	.112
Fulltimetemporary	A	3.995	.046	-1.005	1634	.315	-.008	.008	-.024	.008
	B			-.820	240.361	.413	-.008	.010	-.028	.012
Parttimetemporary	A	.425	.515	-.326	1634	.744	-.003	.008	-.019	.013
	B			-.302	255.465	.763	-.003	.009	-.020	.015
FLSAExemptDummy	A	74.167	.000	-5.606	1634	.000	-.172	.031	-.233	-.112
	B			-4.867	247.063	.000	-.172	.035	-.242	-.103
ZIP_750	A	.252	.616	.250	1634	.803	.006	.023	-.039	.051
	B			.254	270.506	.800	.006	.023	-.039	.050
ZIP_751	A	1.251	.264	-.560	1634	.575	-.003	.006	-.015	.009
	B			-.477	244.739	.634	-.003	.007	-.018	.011
ZIP_752	A	.246	.620	.248	1634	.804	.001	.006	-.010	.013
	B			.272	286.799	.786	.001	.005	-.009	.012
ZIP_754	A	4.683	.031	1.076	1634	.282	.006	.005	-.005	.016
	B			2.835	1429.000	.005	.006	.002	.002	.009
ZIP_760	A	1.238	.266	.554	1634	.580	.006	.010	-.015	.026
	B			.624	292.860	.533	.006	.009	-.012	.024
ZIP_761	A	.107	.744	.163	1634	.870	.002	.009	-.017	.020
	B			.169	274.006	.866	.002	.009	-.016	.019
ZIP_762	A	1.531	.216	-.607	1634	.544	-.017	.027	-.070	.037
	B			-.627	273.322	.531	-.017	.026	-.069	.036
A - Equal variance assumed.										
B - Equal variance not assumed.										

REFERENCE LIST

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2005). *Attitudes, personality and behavior* (2nd ed.). New York: Open University Press.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., & Radosevich, M. (1979). Social learning and deviant behavior: A specific test of a general theory. *American Sociological Review*, 636–655.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276–289.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476–490. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404809000029

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective Reflection. An intervention study. *Computers & Security*, *29*(4), 432–445.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–A15. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=52546047&scope=site

APWG. (2013). *Global phishing survey: Trends and domain name use in 1h2013*. Retrieved from http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf

Awareness. (2013). *Merriam-Webster.com (online)*. Retrieved from http://www.merriam-webster.com/dictionary/awareness

Ball, R. A., Lilly, J. R., & Cullen, F. T. (2010). *Criminological theory: Context and consequences*. Thousand Oaks, Sage Publications, Incorporated.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122–147. doi:10.1037/0003-066x.37.2.122

Bandura, A. (2004). Social cognitive theory for personal and social change by enabling media. In A. Singhal, M.J. Cody, E.M. Rogers, M. Sabido, *Entertainment-education and social change: History, research, and practice* (pp. 75–96). Mahwah, NJ: Lawrence Erlbaum Associates, Inc.

Bandura, A. (2010). Self-efficacy. In t*he Corsini encyclopedia of psychology*. New York: John Wiley & Sons, Inc. doi:10.1002/9780470479216.corpsy0836

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173–82. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/3806354

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, *1*(2), 121–130. doi:10.1057/ejis.1991.20

Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models. *Long Range Planning*, *45*(5-6), 359–394. doi:10.1016/j.lrp.2012.10.001

Bhattacherjee, A. (2012). *Social science research: principles, methods, and practices* (2nd ed.).

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164.

Bosworth, S., & Jacobson, R. V. (2002). Brief history and mission of information system security. In S. Bosworth & R. V Jacobson, *Computer security handbook* (4th ed.). New York: John Wiley & Sons.

Boyle, R. J., & Panko, R. R. (2013). *Corporate computer and network security* (3rd ed.). Upper Saddle River, NJ: Pearson Education.

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

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy & Security*, *1*(3), 18–41. doi:10.2307/3151312

Chang, K., & Wang, C. (2011). Information systems resources and information security. *Information Systems Frontiers*, *13*(4), 579–593. Retrieved from http://dx.doi.org/10.1007/s10796-010-9232-6

Chen, C. C., Shaw, R. S., & Yang, S. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning & Performance Journal*, *24*(1), 1–14.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for Business Research* (pp. 295–358). Lawrence Erlbaum Associates.

Ciampa, M. (2010). *Security awareness: Applying practical security in your world* (3rd ed.). Boston, MA: Course Technology.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211. Retrieved from http://www.jstor.org/stable/249688

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404806001556

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. In *43rd Hawaii International Conference on System Sciences* (pp. 1–10).

Culnan, M. J., Foxman, E. R., & Ray, A. W. (2008). Why it executives should help employees secure their home computers. *MIS Quarterly Executive*, *7*(1), 49–56. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=33160298&site=ehost-live&scope=site

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Commun. ACM*, *50*(10), 113–117. doi:10.1145/1290958.1290971

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of is security countermeasures. *Journal of Business Ethics*, *89*, 59–71. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=38593079&site=ehost-live&scope=site

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=37329141&site=ehost-live&scope=site

Darke, P. R., Chaiken, S., Bohner, G., Einwiller, S., Erb, H.-P., & Hazlewood, J. D. (1998). Accuracy motivation, consensus information, and the law of large numbers: Effects on attitude judgment in the absence of argumentation. *Personality and Social Psychology Bulletin*, *24*(11), 1205–1215. doi:10.1177/01461672982411007

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=4679168&site=ehost-live&scope=site

Deloitte. (2012). Deloitte 2012 TMT global security survey. Retrieved from http://www.deloitte.com/assets/Dcom-Global/Local Assets/Documents/TMT/dttl_TMT 2011 Global Security Survey_High res_191111.pdf

Department of Homeland Security. (2013). Cybersecurity: What every CEO should be asking. Retrieved from http://www.us-cert.gov/security-publications/Cybersecurity-What-Every-CEO-Should-Be-Asking

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, *7*(4), 171–175. Retrieved from https://libproxy.library.unt.edu/login?url=http://search.proquest.com/docview/212313333?accountid=7113

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=26361362&site=ehost-live&scope=site

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, *26*(1), 73–80. doi:http://dx.doi.org/10.1016/j.cose.2006.10.009

Dowland, P. S., Furnell, S., Illingworth, H. M., & Reynolds, P. L. (1999). Computer crime and abuse: A survey of public attitudes and awareness. *Computers & Security*, *18*(8), 715–726.

Drolet, A. L., & Morrison, D. G. (2001). Do we really need multiple-item measures in service research? *Journal of Service Research*, *3*(3), 196–204. doi:10.1177/109467050133001

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review*, *24*(3), 349–375.

Ellen, P. S., Wiener, J. L., & Cobb-Walgren, C. (1991). The role of perceived consumer effectiveness in motivating environmentally conscious behaviors. *Journal of Public Policy & Marketing*, *10*(2), 102–117.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. Retrieved from http://hfs.sagepub.com/content/37/1/32.abstract

Endsley, M. R., Bolté, B., & Jones, D. G. (2003). *Designing for situation awareness. An approach to user-centred design* (1st ed.). Boca Raton, FL: CRC Press.

Endsley, M. R., & Garland, D. J. (2000). *Situation awareness analysis and measurement*. Mahwah, NJ: Lawrence Erlbaum Associates.

Feinberg, M., Greenberg, M., & Osgood, D. W. (2004). Readiness, functioning, and perceived effectiveness in community prevention coalitions: A study of communities that care. *American Journal of Community Psychology*, *33*(3-4), 163–176. doi:10.1023/B:AJCP.0000027003.75394.2b

Fishbein, M., Hall-Jamieson, K., Zimmer, E., von Haeften, I., & Nabi, R. (2002). Avoiding the boomerang: Testing the relative effectiveness of antidrug public service announcements before a national campaign. *American Journal of Public Health*, *92*(2), 238–245. doi:10.2105/AJPH.92.2.238

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: algebra and statistics. *Journal of Marketing Research (JMR)*, *18*(3), 382–388. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=5012893&site=ehost-live&scope=site

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, *24*(4), 274–279.

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

Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to sem guidelines for administrative and social science research. *MIS Quarterly*, *35*(2), iii–A7.

Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika*, *61*(1), 101–107. Retrieved from http://biomet.oxfordjournals.org/content/61/1/101.short

Goncharov, M. (2012). Russian Underground 101. Trend Micro Incorporated. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Goodhue, D. L., & Straub, D. W. (1989). Security concerns of system users: a proposed study of user perceptions of the adequacy of security measures. In *System Sciences, 1989. Vol.IV:*

Emerging Technologies and Applications Track, Proceedings of the Twenty-Second Annual Hawaii International Conference on System Sciences (Vol. 4, pp. 117–127 vol.4).

Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, *13*(4), 29–47. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=1813573&scope=site

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203–236. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=67194187&site=ehost-live&scope=site

Hagen, J. M., Albrechtsen, E., & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security*, *19*(3), 140–154.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage Publications, Inc.

Henseler, J., & Chin, W. W. (2010). A comparison of approaches for the analysis of interaction effects between latent variables using partial least squares path modeling. *Structural Equation Modeling: A Multidisciplinary Journal*, *17*(1), 82–109. doi:10.1080/10705510903439003

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In R. R. Sinkovics & P. N. Ghauri, *Advances in International Marketing* (Vol. 20, pp. 277–320). Bingley: Emerald.

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

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

Herold, R. (2010). *Managing an information security and privacy awareness and training program*. Boca Raton: FL, CRC Press.

Hirschi, T. (2002). *Causes of delinquency*. Piscataway, NJ: Transaction Pub.

Ho, R. (2014). *Handbook of univariate and multivariate data analysis with ibm spss* (2nd ed.). Boca Raton, FL: CRC Press.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74. doi:10.1145/2063176.2063197

Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870–883. Retrieved from http://www.sciencedirect.com/science/article/pii/S1071581911001029

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. doi:http://dx.doi.org/10.1016/j.cose.2011.10.007

Information Assurance Support Environment. (2013). Phishing awareness 2.0. Retrieved from http://iase.disa.mil/eta/phishing_v2/phishing_v2/launchPage.htm

ISO/IEC. (2005). ISO/IEC 17799:2005(E) Information Technology —— Security Techniques —— Code of Practice for Information Security Management. Geneva, Switzerland: ISO/IEC.

James, L. (2009). *Phishing Exposed*. Rockland, MA: Syngress.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–A4. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=52546360&site=ehost-live&scope=site

Judd, C. M., & Kenny, D. A. (1981). Process analysis: Estimating mediation in treatment evaluations. *Evaluation Review*, *5*(5), 602–619. doi:10.1177/0193841X8100500502

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

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (is) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=67093418&scope=site

Kaspersky Labs. (2013). Spam statistics report Q2-2013. Retrieved October 03, 2014, from http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q2-2013#.Ux4jwfldXNk

Keil, M., Tan, B. C. Y., Wei, K., Saarinen, T., & Tuunainen, V. (2000). A cross-cultural study on escalation of commitment behavior in software projects. *Mis Quarterly*, *24*(2), 299–325. Retrieved from http://www.jstor.org/stable/3250940

Kerlinger, F. N., & Lee, H. B. (2000). *Foundations of behavioral research* (4th ed.). Belmont, CA: Cengage Learning.

Kihlstrom, J. F., & Cantor, N. (1984). Mental representations of the self. In R. Berkovitz (Ed.), *Advances in experimental Social Psychology Volume 17* (Vol. 17, pp. 1–47). Orlando, FL: Academic Press, Inc. doi:10.1016/S0065-2601(08)60117-3

Kirsch, L., & Boss, S. (2007). The last line of defense : motivating employees to follow corporate security guidelines information privacy and security abstract. In *ICIS 2007 Proceedings. Paper 103*. Montreal. Retrieved from http://aisel.aisnet.org/icis2007/103/

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5–6), 224–231. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404808000321

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, *46*(1), 254–264. Retrieved from http://www.sciencedirect.com/science/article/B6V8S-4SY6W1D-1/2/7f5792408e6fc7775cd5e005083daec8

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Commun. ACM*, *51*(3), 71–76. doi:10.1145/1325555.1325569

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. New York: Springer Publishing Company.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, *10*(2), 57–63.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707–718. doi:http://dx.doi.org/10.1016/j.im.2003.08.008

Lee, Y., & 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), 177–187. Retrieved from http://dx.doi.org/10.1057/ejis.2009.11

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=36527735&site=ehost-live&scope=site

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=56503617&scope=site

Lininger, R., & Vines, R. D. (2005). *Phishing. Cutting the identity theft line*. Indianapolis, Indiana: Wiley Publishing, Inc.

Lombroso, C. (1911). *Crime, its causes and remedies* (Vol. 3). Boston, MA: Little Brown.

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin*, *18*(1), 3–9. doi:10.1177/0146167292181001

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. Retrieved from http://www.sciencedirect.com/science/article/B6WJB-4D60J0Y-21/2/1c52a5609d22304be21325289450cdd9

Mallery, J. (2009). Building a secure organization. In J. R. Vacca (Ed.), *Computer and Information Security Handbook* (pp. 3–21). Burlington, MA: Morgan Kaufmann. doi:http://dx.doi.org/10.1016/B978-0-12-374354-1.00001-7

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science*, *34*(5), 583–598. Retrieved from http://www.jstor.org/stable/2632080

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. doi:10.1111/j.1559-1816.2000.tb02308.x

Mooi, E. A., & Sarstedt, M. (2011). *A concise guide to market research: The process, data, and methods using IBM SPSS Statistics*. Berlin: Springer.

Myers, S. (2007). Introduction to phishing. In M. Jakobsson & S. Myers (Eds.), *Phishing and Countermeasures* (pp. 1–30). New York: John Wiley & Sons, Inc.

National Institute of Standards and Technology. (1998). NIST special publication 800-16 - information technology security training requirements: A role-and performance-based model. http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

National Institute of Standards and Technology. (2003). NIST special publication 800-50 - Building an information technology security awareness and training program. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. Retrieved from http://www.sciencedirect.com/science/article/B6V8S-4TYYMNV-3/2/842f546339406093d3e1fb6c28e5ef71

O'Leary, M. B., & Cummings, J. N. (2007). The spatial, temporal, and configurational characteristics of geographic dispersion in teams. *MIS Quarterly*, *31*(3), 433–452. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=25990742&scope=site

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards is security policy compliance. In *40th Annual Hawaii International Conference on System Sciences*. Waikoloa, HI: IEEE Computer Society.

Pavlou, P. A., Huigang, L., & Yajiong, X. (2007). Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. *MIS Quarterly*, *31*(1), 105–136. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=23963781&site=ehost-live&scope=site

Podsakoff, P. M., MacKenzie, S. B., Jeong-Yeon, L., & 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), 879. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=10986397&site=ehost-live&scope=site

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 767–A4. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=54990496&site=ehost-live&scope=site

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7-8), 241–253.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826. doi:10.1016/j.cose.2009.05.008

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221–232. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404811001441

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0. www.smartpls.de. Retrieved from http://www.smartpls.com

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=5194756&site=ehost-live&scope=site

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Ciacioppo & R. Petty (Eds.), *Social Psychophysiology*. New York: Guilford Press.

Rosenstock, I. M. (1974). The health belief model and preventive health behavior. *Health Education & Behavior*, *2*(4), 354–386. doi:10.1177/109019817400200405

Rossiter, J. R. (2002). The C-OAR-SE procedure for scale development in marketing. *International Journal of Research in Marketing*, *19*(4), 305–335. doi:10.1016/S0167-8116(02)00097-6

Rudolph, K., Warshawsky, G., & Numkin, L. (2002). Security awareness. In S. Bosworth & M. E. Kabay (Eds.), *Computer Security Handbook* (4th ed., pp. 29.1–29–19). New York, NY: John Wiley & Sons, Inc.

SANS Institute. (2013). Security awareness planning. Retrieved January 06, 2013, from http://www.securingthehuman.org/resources/planning

Saran, C. (2013). Enterprises abandon Java due to securtyy holes. ComputerWeekly. Retrieved from http://www.computerweekly.com/news/2240181037/Enterprises-abandon-Java-due-to-security-holes

Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multigroup analysis in partial least squares (PLS) path modeling: alternative methods and empirical results. *Advances in International Marketing, 22*, 195–218. doi:10.1108/S1474-7979(2011)0000022012

Sarter, N., & Woods, D. (1991). Situation awareness: A critical but ill-defined phenomenon. *The International Journal of Aviation Psychology*, *1*(1), 45–57. Retrieved from http://www.tandfonline.com/doi/abs/10.1207/s15327108ijap0101_4

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link" -- a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, *19*(3), 122. Retrieved from https://libproxy.library.unt.edu/login?url=http://search.proquest.com/docview/215204902?accountid=7113

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. Retrieved from http://www.sciencedirect.com/science/article/pii/S0360131508001012

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41.

Siponen, M. (2001). Five dimensions of information security awareness. *Computers & Society*, *31*(2), 24–29.

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and is security policy compliance. In *Innovations in Information Technology, 2006* (pp. 1–5).

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Siponen, M., & Vance, A. (2013). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems*. Retrieved from http://dx.doi.org/10.1057/ejis.2012.59

Sophos Group. (2012). Security threat report 2012. Seeing the threats through the hype. Retrieved from http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

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

Spitzner, L. (2013). The top seven human risks - initial findings. *SecuringtheHuman Security Awareness Blog*. SANS Institute. Retrieved from http://www.securingthehuman.org/blog/2013/02/21/the-top-seven-human-risks-initial-findings

Stamper, R. (1973). *Information in business and administrative systems*. New York: John Wiley & Sons, Inc.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society. Series B (…*, *36*(2), 111–147. Retrieved from http://www.jstor.org/stable/2984809

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276. Retrieved from http://pubsonline.informs.org/doi/abs/10.1287/isre.1.3.255

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=1649969&site=ehost-live&scope=site

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). *Principles of criminology*. Lanham, MD: Altamira Press.

Tabachnick, B. G., & Fidell, L. S. (2001). *Using multivariate statistics* (5th ed.). Boston, MA: Pearson Education.

Talib, S., Clarke, N. L., & Furnell, S. (2010). An analysis of information security awareness within home and work environments. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on* (pp. 196–203).

Taylor, S. E., Wayment, H. A., & Carrillo, M. (1996). Social comparison, self-regulation, and motivation. In R. M. Sorrentino & E. T. Higgins (Eds.), *Handbook of motivation and cognition* (pp. 3–27). New York, NY: Guilford Press.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173.

Tidwell, C. L. (2010). Measuring the effect of using simulated security awareness training and testing on members of virtual communities of practice. *Journal of Systemics, Cybernetics & Informatics*, *8*(6), 85–88. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=60001576&site=ehost-live&scope=site

Todorov, A., Chaiken, S., & Henderson, M. D. (2002). The heuristic-systematic model of social information processing. *The Persuasion Handbook: Developments in Theory and Practice*, 195.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008a). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*, *17*(5/6), 207–227.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008b). Process-variance models in information security awareness research. *Information Management & Computer Security*, *16*(3), 271–287.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198. Retrieved from http://www.sciencedirect.com/science/article/pii/S0378720612000328

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=10758835&site=ehost-live&scope=site

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198. doi:http://dx.doi.org/10.1016/j.cose.2004.01.012

Warkentin, M., & Johnston, A. C. (2008). IT security governance and centralized security controls. In *Information security and ethics: concepts, methodologies, tools, and applications* (pp. 2130–2138). IGI Global. doi:10.4018/978-1-59904-937-3.ch143

Warkentin, M., Malimage, N., & Malimage, K. (2012). Impact of protection motivation and deterrence on is security policy compliance: A multi-cultural view. In *pre-ICIS workshop on Information Security and Privacy (SIGSEC). Paper 20.*

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105.

Weinstein, N. D. (2000). Perceived probability, perceived severity, and health-protective behavior. *Health Psychology*, *19*(1), 65–74. doi:10.1037/0278-6133.19.1.65

West, M. (2009). Preventing system intrusion. In J. R. Vacca (Ed.), *Computer and information security handbook* (1st ed., pp. 39–52). Burlington, MA: Morgan Kaufmann.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Commun. ACM*, *46*(8), 91–95. doi:10.1145/859670.859675

Whitman, M. E., & Mattord, H. J. (2012). *Principles of infomation security* (4th ed.). Boston, MA: Course Technology.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1–20. Retrieved from https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=85640558&scope=site

Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–342. doi:10.1080/108107396127988

Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *Proceedings of the 26th International Conference on Information Systems* (pp. 367–380). Retrieved from http://aisel.aisnet.org/icis2005/31

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. doi:http://dx.doi.org/10.1016/j.chb.2008.04.005