2013

Assessing the Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills toward Computer Misuse Intention at Government Agencies

Min Suk Choi
Nova Southeastern University, krambo@gmail.com

Assessing the Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills toward Computer Misuse Intention at Government Agencies

by

Min Suk Choi

A dissertation submitted in partial fulfillment of the requirement for the degree of
Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2013

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Assessing the Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills toward Computer Misuse Intention at Government Agencies

by
Min Suk Choi
May 2013

Cybersecurity threats and vulnerabilities are causing substantial financial losses for governments and organizations all over the world. Cybersecurity criminals are stealing more than one billion dollars from banks every year by exploiting vulnerabilities caused by bank users' computer misuse. Cybersecurity breaches are threatening the common welfare of citizens since more and more terrorists are using cyberterrorism to target critical infrastructures (e.g., transportation, telecommunications, power, nuclear plants, water supply, banking) to coerce the targeted government and its people to accomplish their political objectives. Cyberwar is another major concern that nations around the world are struggling to get ready to fight. It has been found that intentional and unintentional users' misuse of information systems (IS) resources represents about 50% to 75% of cybersecurity threats and vulnerabilities to organizations. Computer Crime and Security Survey revealed that nearly 60% of security breaches occurred from inside the organization by users.

Computer users are one of the weakest links in the information systems security chain, because users seem to have very limited or no knowledge of user computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS). Users' CSE, CCA, and CS play an important role in users' computer misuse intention (CMI). CMI can be categorized as unauthorized access, use, disruption, modification, disclosure, inspection, recording, or destruction of information system data. This dissertation used a survey to empirically assess users' CSE, CCA, CS, and computer misuse intention (CMI) at government agencies. This study used Partial Least Square (PLS) technique to measure the fit of a theoretical model that includes seven independent latent variables (CSE, UAS-P, UAS-T, UAC-M, CCS, CIS, & CAS) and their influences on the dependent variable CMI. Also, PLS was used to examine if the six control variables (age, gender, job function, education level, length of working in the organization, & military status such as veteran) had any significant impact on CMI.

This study included data collected from 185 employees of a local and state transportation agency from a large metropolitan in the northeastern United States. Participants received an email invitation to take the Web-based survey. PLS was used to test the four research hypotheses. The results of the PLS model showed that UAC-M and CIS were significant contributors ($p < .05$) to CMI. UAC-M was a significant contributor ($p < .05$) to CCS. UAS-P was a significant contributor ($p < .05$) to CAS. CSE was the most significant contributor ($p < .001$) to CCS, while it did not show a significance contribution towards CMI. It can be concluded that UAC-M and CIS play a significant role on CMI. This investigation contributes to the IS and cybersecurity practice by providing valuable information that can be used by government agencies in an effort to significantly reduce computer users' abuse, while increasing productivity and effectiveness.

ACKNOWLEDGEMENTS

I would like to dedicate this to God for his unconditional love and guidance. To my mother who introduced me to God and showed me that everything is possible with faith and hard work. My two sisters and brother for their prayers, love, and support. To my wife Soojin, kids Dahae, Joohee, Isaac, and Joseph for all the love and joy in my life.

Special thanks to my advisor, Dr. Yair Levy, for his leadership, guidance, and support throughout this rigorous dissertation process. I have learned so much from Dr. Levy. I also want to thank my committee members, Dr. Anat Zeelim-Hovav and Dr. William L. Hafner for all their helpful comments and support throughout this process. I like to thank Dr. Ling Wang for helping me with IRB.

Finally, I would like to express my appreciation to Tariq, Steven, Deborah, Jerome, Anthony, Chuck, and others for helping me with the survey.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1
Introduction

Background

The fast growing cybersecurity threats and vulnerabilities are causing substantial financial losses for governments and organizations all over the world (The White House, 2009). Cyber-attacks, hacking, and computer misuse by employees are costing millions of dollars to organizations around the world every day (Gal-Or & Ghose, 2005). Cybersecurity breaches have increased rapidly over the years, and they continue growing at an alarming rate (Veiga & Eloff, 2007). One of the biggest challenges nowadays in cybersecurity is the behavior of users due to their limited cybersecurity skills (Thomson & Solms, 2005). Thus, this study focused on assessing the role of user computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) toward computer misuse intention (CMI) at government agencies.

CSE, CCA, and CS were found to play an important role in reducing CMI, human error in data processing, information theft, digital fraud, and misuse of computer assets in organizations (D'Arcy, Hovav, & Galletta, 2009; Drevin, Kruger, & Steyn, 2007). It appears that users are one of the weakest links in the information systems (IS) security chain, because users seem to have very limited or no knowledge of CSE, CCA, and CS (Albrechtsen, 2007; Clifford, 2008). CSE, CCA, and CS are essential in educating and developing users' awareness and skills to help reduce cybersecurity vulnerabilities such as CMI (Clifford, 2008; D'Arcy et al., 2009).

The structure of this document is in the following order. Problem statement, dissertation/research goal, research questions, relevance and significance of the study, brief review of the literature, barriers and issues, approach, results, conclusions, implications, recommendations, summary, resources, and references.

Problem Statement

The research problem that this study addressed was the fast growing cybersecurity threats and vulnerabilities from users' computer misuse that are causing substantial financial losses for governments and organizations all over the world (Blanke, 2008; D'Arcy et al., 2009; Gal-Or & Ghose, 2005). Axelrod (2006) defined cybersecurity as "the prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems to ensure confidentiality, integrity and availability" (p. 1). Cyber-attacks, hacking, and computer misuse by users (e.g., employees, consultants, contractors, & business partners) are costing millions of dollars to organizations around the world every day (Gal-Or & Ghose, 2005). Torkzadeh and Lee (2003) defined users as "individuals who may use codes written by others" (p. 608). Computer users are individuals that interact or use computer software applications in order to perform their work or achieve their intended actions, while do not write computer code on their own (Torkzadeh & Lee, 2003). Straub (1990) defined computer misuse as "unauthorized deliberate and internally recognizable misuse of assets of the local organizational information system by individuals" (p. 527). D'Arcy et al. (2009) defined computer misuse intention as an "individual's intention to perform a behavior that is defined by the organization as a misuse of IS resources" (p. 81).

Cybersecurity criminals are stealing more than one billion dollars from banks every year by exploiting vulnerabilities caused by bank users’ computer misuse (Farrell & Riley, 2011). It has been found that intentional and unintentional users' misuse of information systems resources represents about 50% to 75% of cybersecurity threats and vulnerabilities to organizations (D’Arcy et al., 2009). D’Arcy and Hovav (2007) claimed that users’ computer misuse is a very serious problem for organizations. Users’ computer misuse includes sending inappropriate emails using their organization’s email, installation of unlicensed and unauthorized computer software, unauthorized modification of computerized data, access to unauthorized computers, password sharing, and password stealing. Blanke (2008) found that users’ computer misuse is one of the biggest cybersecurity issues in organizations all over the world. According to a survey by Ernst and Young, security incidents can cost companies between $17 and $28 million for each occurrence (Veiga & Eloff, 2007). The 2010/2011 Computer Crime and Security Survey (2011) revealed that approximately 59.1% of security breaches occurred from inside the organization by users. A White House report (2009) that addressed the systemic loss of United States (U.S.) economic value estimated that in 2008 alone the loss from intellectual property to data theft was up to one trillion dollars. Cybersecurity breaches have increased rapidly over the years and they continue growing at an alarming rate (Veiga & Eloff, 2007). One of the biggest challenges nowadays in cybersecurity is the behavior of users due to the user’s limited cybersecurity skills (Thomson & Solms, 2005). Yet, limited work has been done to study cybersecurity skills, let alone to develop viable instruments to measure such skills.

Government agencies are not exempt from cybersecurity attacks and vulnerabilities caused by users' computer misuse. According to Clarke and Knake (2010), several government agencies have been hit by cybersecurity attacks. Many U.S. government agencies such as the Central Intelligence Agency (CIA), Department of Defense (DoD), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and Federal Aviation Administration (FAA) are few examples of agencies that have been attacked by cybercriminals recently (Clarke & Knake, 2010; Rosenzweig, 2012). In addition, cybersecurity breaches are threatening the common welfare of citizens since more and more terrorists are using cyberterrorism to target critical infrastructures (e.g., transportation, telecommunications, power, nuclear plants, water supply, banking) to terrorize and coerce the targeted government and its people to accomplish their political objectives (Foltz, 2004). Terrorist organizations can easily hire outside hackers and users from the targeted organization to work for them (Foltz, 2004). Foltz (2004) defined cyberterrorism as "concerted, sophisticated attacks on networks" (p. 154). Cyberwar is another major concern that nations around the world are struggling to get ready to fight (Clarke & Knake, 2010). Clarke and Knake (2010) defined cyberwar as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (p. 6). Cybersecurity has become one of the top priorities of the U.S. government (The White House, 2009). President Obama mandated a comprehensive review to assess the national cybersecurity policies and structures in order to evaluate the ever increasing cybersecurity attacks, system vulnerabilities, and information system misuse (The White House, 2009). It is important to understand that cybersecurity criminals, cyber-terrorists, and cyber-warriors are exploiting and hacking into IS vulnerabilities that are often caused by users' intentional and unintentional computer misuse (Blanke 2008; Clarke & Knake, 2010).

Users' computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) play an important role in users' computer misuse intention (CMI) (Blanke, 2008; D'Arcy et al., 2009; Ruighaver, Maynard, & Chang, 2007). Compeau and Higgins (1995) defined self-efficacy "as beliefs about one's ability to perform a specific behavior" (p. 146). Computer self-efficacy pertains to individuals' judgment of their capabilities to use computers in various situations to perform a task successfully (Compeau & Higgins, 1995; Chau, 2001; Marakas, Yi, & Johnson, 1998). Compeau and Higgins (1995) claimed that studies have uncovered a close relationship between self-efficacy, skill, and individual behaviors regarding technology usage and adoption. Skill is the combined knowledge, ability, and experience that allow an individual to successfully perform an action, while computer self-efficacy (CSE) is the perception of the ability to successfully perform an action using a computer (Compeau & Higgins, 1995; McCoy, 2010). Chan, Woon, and Kankanhalli (2005) conducted a study based on Compeau and Higgins' (1995) CSE focusing on breaches in information security. Chan et al. (2005) found that users' perception of CSE and the organization's cybersecurity view positively impact their compliant behavior. Their study concluded that compliant behavior can be promoted by increasing users' CSE and enhancing awareness of the importance of cybersecurity to them and their organization (Chan et al., 2005). D'Arcy and Hovav (2009) stated that "research that has examined risky decision making among various groups suggests that there is a significant relationship between perceptions of self-efficacy and risk-taking behavior" (p. 61). Wyatt (1990) found several risky behaviors (e.g., computer misuse) among college students and stated that self-efficacy was the principle variable influencing risk-taking behavior. D'Arcy and Hovav (2009) found that self-efficacy influences risk-taking behavior through opportunity recognition. They suggested that CSE appears to have different effects depending on the computer misuse activity (i.e., ones that apply to computer savvy users & ones that apply to computer non-savvy users). CCA comprises user awareness of security policy, security-training programs, computer monitoring, and computer sanctions (Aakash, 2006; D'Arcy et al., 2009). D'Arcy et al.'s (2009) study found that cybersecurity countermeasures such as the four aforementioned dimensions of user security and computer awareness are each effective in discouraging users' CMI. Users' computer misuse is a serious and very costly threat to an organization's financial stability (D'Arcy & Hovav, 2007). Although, the aforementioned studies have focused on addressing CMI, these studies have not investigated the role of skills, specifically cybersecurity skills, into their model.

Users are one of the weakest links in the IS security chain because many users appear to have limited or no cybersecurity skills (Albrechtsen, 2007; Clifford, 2008). Most users do not understand the importance of protecting computer information systems, and this lack of understanding is reflected in their negligence in cybersecurity practices (Thomson & Solms, 2005). Users cannot be held responsible for cybersecurity problems if they are not educated and trained to acquire the right skills to be able to identify what such security problems are as well as what they should do to prevent them (Solms & Solms, 2004). Boyatzis and Kolb (1991) defined skill as a "combination of ability, knowledge and experience that enables a person to do something well" (p. 280).

Skill is the ability to understand and make use of different intellectual abilities (i.e. knowledge), combined with the individual's prior experience to achieve the most appropriate action for the best result. For example, the combined ability, knowledge, and experience to install, configure, and/or maintain antivirus software to protect the operating systems of a computer is a type of a computer skill (Levy, 2005; Torkzadeh & Lee, 2003). For most users, a computer system is a tool to perform their job responsibilities as efficiently as possible, while they view cybersecurity as a barrier rather than a necessity due to their lack of cybersecurity skills (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2006).

CSE, CCA, and CS all play an important role in reducing CMI, human error in data processing, information theft, digital fraud, and misuse of computer assets in organizations (D'Arcy et al., 2009; Drevin et al., 2007). Although all of CCA's user awareness of security policy (UAS-P), user awareness of security-training programs (UAS-T), user awareness of computer monitoring (UAC-M), and user awareness of computer sanctions (UAC-S) play a key role in reducing users' CMI in their organizations (D'Arcy et al., 2009; Ruighaver et al., 2007), D'Arcy et al. (2009) suggested that perceived severity of sanctions appear to have a significant direct effect on users' CMI. Unfortunately, organizations are reluctant to invest in CCA programs due to their lack of knowledge of the cybersecurity risks and cost associated with implementing CCA programs (Ruighaver et al., 2007). Thomson and Solms (2005) claimed that cybersecurity should become second nature behavior in users' daily activity in order to help reduce their computer misuse. Increasing CCA appears to increase users' perceptions of the negative impact that computer misuse could cause to their organization

(D’Arcy et al., 2009; Thomson & Solms, 2005). CCA is essential in educating and developing users’ cybersecurity skills to help reduce cybersecurity vulnerabilities (Clifford, 2008; D’Arcy et al., 2009). While significant research has been done in the cybersecurity domain, very little attention has been given to the study of user CMI (D’Arcy et al., 2009; Torkzadeh & Lee, 2003). According to Ajzen (1989), behavioral intention is the individual’s intention to perform or not perform a specific behavior. Based on Ajzen’s definition and for the purpose of this study, CMI is defined as a user’s intention to perform computer misuse. A user’s CMI is the indicator that the individual may have the behavioral intention to use the computer to commit computer misuse in his or her organization and negatively affect cybersecurity. Government agencies are under a lot of pressure to improve cybersecurity (The White House, 2009). Thus, it appears that additional empirical investigation on the role of computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) towards computer misuse intention (CMI) is necessary since cybersecurity plays a crucial part of the world’s economy, infrastructure, and military today (Clarke & Knake, 2010; D’Arcy et al., 2009).

Research Goals

The main goal of this research study was to empirically test a predictive model on the impact of computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) on computer misuse intention (CMI) at government agencies. The need for this study is demonstrated by D’Arcy et al.’s (2009) study on user awareness of security countermeasures and its impact on information systems misuse;

Blanke's (2008) research on employee's intention to commit computer misuse in business environments; Aakash's (2006) research on antecedents of information system exploitation in organizations; as well as Torkzadeh and Lee's (2003) study on the measures of user computing skills. D'Arcy et al. (2009) claimed that intentional and unintentional insider misuse of information systems resources (i.e., computer misuse) represents a significant threat to organizations. Blanke (2008) indicated that American businesses alone will lose around $63 billion each year due to employees' computer misuse. Aakash (2006) pointed out that organizations should invest in cybersecurity awareness programs, education, training, and sanctions to increase employees' cybersecurity compliance. Torkzadeh and Lee (2003) reported on the need to develop a measuring instrument to properly assess user computing skills. Unfortunately, limited numbers of research studies have been done on CSE, CCA, and CS toward CMI (Blanke, 2008; Clarke & Knake, 2010; D'Arcy et al., 2009). D'Arcy et al. (2009) stated that users' computer misuse is the source of 50% to 75% of security incidents. Therefore, an investigation on user's CMI appears to be warranted.

This study focused on three key independent variables (CSE, CCA, & CS constructs) as potential predictors for CMI as described in Figure 1. The theoretical foundation is based on general deterrence theory (GDT). GDT posits that individuals can be dissuaded from committing antisocial acts through the use of countermeasures, which include strong disincentives and sanctions relative to the act (Straub & Welke, 1998). For example, due to the lack of cybersecurity skills training and sanctions, an organizational user may fail to follow procedures, which leads to data loss, destruction, or a failure of data integrity (Straub & Welke, 1998).

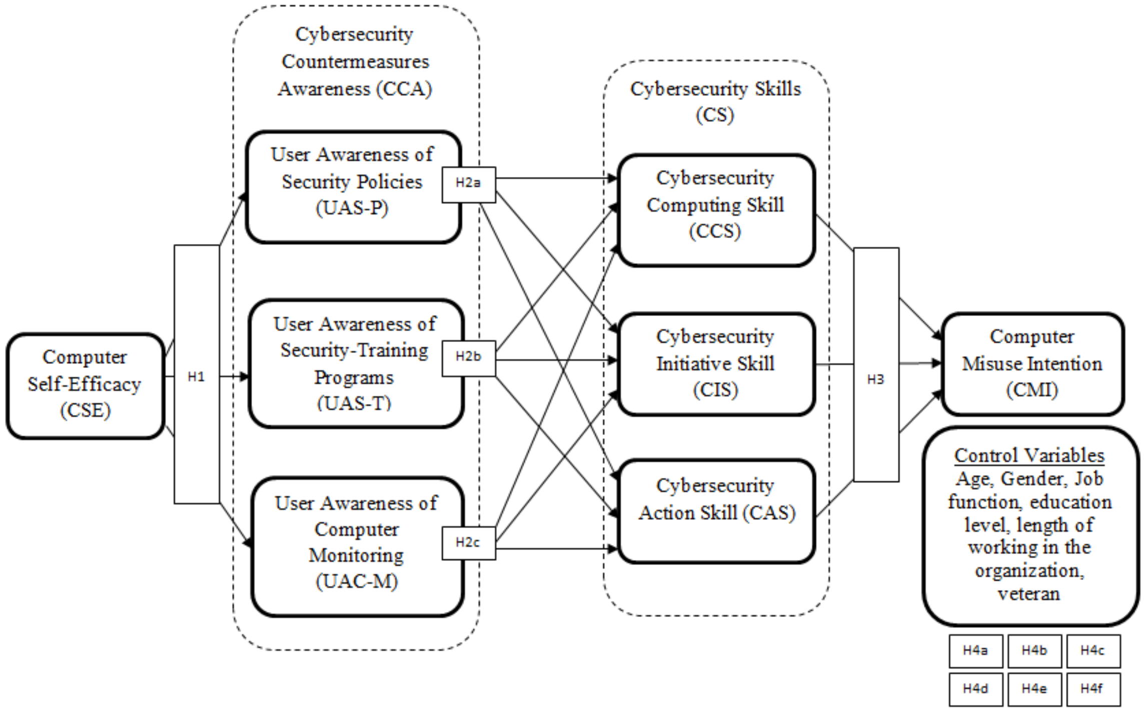

Figure 1. The CMI conceptual research map based on GDT

Cybersecurity computing skill (CCS), cybersecurity initiative skill (CIS), and cybersecurity action skill (CAS) are considered as the three major facets of users' cybersecurity skill (CS) (Aakash, 2006; Blanke, 2008; Levy, 2005; Torkzadeh & Lee, 2003). Levy (2005) defined computing skill as the "ability to use computers and computer networks to analyze data and organize information" (p. 6). He also defined initiative skill as the "ability to seek out and take advantage of opportunities" (p. 6). Levy (2005) defined action skill as the "ability to commit to objectives, to meet deadlines" (p. 6). Accordingly, the cybersecurity computing skill was defined in this research as the ability to use protective tools (e.g., encryption) to protect computers and computer networks to secure data and information systems. The cybersecurity initiative skill was defined as the ability to seek out and take advantage of security software (e.g., antivirus program) and best practices. Lastly, the cybersecurity action skill was defined as the ability to commit to objectives and to meet security compliance (e.g., laptop encryption). The three facets (i.e., CCS, CIS, & CAS) of users' cybersecurity skill are important since a user needs to have adequate levels of these three cybersecurity skills combined in order to demonstrate appropriate overall cybersecurity skill (Aakash, 2006; Blanke, 2008; Levy, 2005; Torkzadeh & Lee, 2003). Computer misuse can be described as unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational IS by individuals, including violations against hardware, programs, data, and computer service (Straub, 1986).

This research was built on previous studies conducted by D'Arcy et al. (2009), Levy (2005), Blanke (2008), Torkzadeh and Lee (2003), as well as Aakash (2006), by investigating the contributions of users' CSE, CCA, and CS toward CMI in an attempt to validate a model to assess users' CMI in a government agency. The first specific goal of this study was to empirically assess CSE and its contribution to CCA dimensions. The second goal of this study was to empirically assess CCA dimensions and its contribution to CS. The third goal of this study was to empirically assess CS and its contribution to CMI. The fourth goal of this study was to empirically assess the contribution of the six control variables: age, gender, job function (i.e., officer, security operator, managerial, operations, technical, professional staff, and administrative staff), education level, length of working in the organization, and military status (e.g., veteran) to CMI. The last goal was to empirically assess the fit of the model by using CCA (i.e., UAS-P, UAS-T, & UAC-M), CCA (i.e., UAS-P, UAS-T, & UAC-M), CS (i.e., CCS, CIS, & CAS), CMI, and control variables.

The four hypotheses that this study addressed are:

H1: Computer self-efficacy (CSE) of users will show significant positive influence on the cybersecurity countermeasures awareness dimensions (UAS-P, UAS-T, & UAC-M).

H2a: User awareness of security policy (UAS-P) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H2b: User awareness of security-training programs (UAS-T) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H2c: User awareness of computer monitoring (UAC-M) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H3: The three cybersecurity skills (CCS, CIS, & CAS) of users will show significant negative influence on Computer Misuse Intention (CMI).

H4a: Users' *age* will show no significant influence on Computer Misuse Intention (CMI).

H4b: Users' *gender* will show no significant influence on Computer Misuse Intention (CMI).

H4c: Users' *job function* will show no significant influence on Computer Misuse Intention (CMI).

H4d: Users' *education level* will show no significant influence on Computer Misuse Intention (CMI).

H4e: Users' *length of working in the organization* will show no significant influence on Computer Misuse Intention (CMI).

H4f: Users' *military veteran status (i.e. 'yes' or 'no')* will show no significant influence on Computer Misuse Intention (CMI).

Relevance and Significance

Relevance of this Study

There are many protective technologies, such as firewall, antivirus software, and instruction detection systems implemented in organizations to protect them from computer misuse (Dinev, Goo, Hu, & Nam, 2008). These protective technologies, which are designed to protect users from computer viruses, spyware, worms, and other malware (e.g., hacking tools), suffer from many complexities and vulnerabilities such as lack of proper software configuration and updates (Dinev et al., 2008). It appears that information security practitioners and managers pay more attention to protective technologies to mitigate security threats than to the security risks caused by users due to the lack of cybersecurity training and/or skills (Rezgui & Marks, 2008). Rezgui and Marks (2008) defined information security as "the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use" (p. 243). They also defined risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets" (Rezgui & Marks, 2008, p. 243).

Users play a large role in information security (Veiga & Eloff, 2007). Many users are complacent about potential computer security risks when protective technologies (e.g., antivirus software) are not used or installed in their computer. They are willing to accept the security risks rather than addressing them due to the nuisances caused by security measures and cost (Dinev et al., 2008). It appears that fighting effectively against information security risks caused by malicious and harmful applications (e.g., viruses, worms, spyware, or malware) cannot be solely accomplished by using protective information technologies (IT). Therefore, assessing the role of user CSE, CCA, and CS toward CMI seems to be warranted (Blanke, 2008; D'Arcy et al., 2009; Dinev et al., 2008; Torkzadeh & Lee, 2003). Dinev et al. (2008) claimed that a "computer user that is aware of the security threats of spyware will be more motivated to use an anti-spyware" (p. 8). The relevance of this study to the fast growing cybersecurity threats and vulnerabilities is by assessing the role of user CSE, CCA, and CS toward CMI. According to the White House (2009), cybersecurity awareness, education, and training are important to develop users' cybersecurity skills in digital safety, ethics, and security to protect them from ever increasing cybersecurity attacks. This study provides measurable data to cybersecurity practitioners and IT managers. This study helps cybersecurity practitioners and IT managers justify funding for cybersecurity programs for end users' cybersecurity skill development. In addition, this study contributes to the research community by providing its findings for further research; this study also expands the body of knowledge (BoK) in the area of user CSE, CCA, and CS roles toward CMI (Besnard & Arief, 2004; Blanke, 2008; D'Arcy et al., 2009; Dinev et al., 2008; Rezgui & Marks, 2008; Torkzadeh & Lee, 2003; Veiga & Eloff, 2007; White House, 2009).

Significance of this Study

The 2010/2011 Computer Crime and Security Survey (2011) revealed that approximately 59.1% of security breaches occurred from inside the organization by users. More than 77% of computer attacks originate in the form of users' computer misuse as they activate viruses and worms embedded in emails and pirated software (e.g., songs, movies, games, or applications) they obtain (Chan et al., 2005). Constantly, users computer misuse, international terrorists, hackers, and cyber-criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government with the intentions to compromise, steal, change, or completely destroy information (The White House, 2009). Organizations are losing millions of dollars every day due to cybersecurity breaches (The White House, 2009). Today, cybersecurity has a direct impact on and is a threat to the nations' security; cyberwar is a reality not science fiction anymore (Clarke & Knake, 2010).

It appears that intentional and unintentional user computer misuse is one of the greatest cybersecurity threats and vulnerabilities to organizations (Blanke, 2008; D'Arcy et al., 2009). Cybersecurity threats are on a steady rise, thus, the U.S. government is constantly increasing the number of professionals to mitigate cybersecurity threats in both public and private sectors (The White House, 2009). One of the U.S. government's top priorities is to promote cybersecurity risk awareness for its citizens and build an education system that will enhance understanding of cybersecurity (The White House, 2009). The significance of this study stem from the results of the assessment on the role of users' CSE, CCA, and CS toward CMI at government agencies, as well as the investigation of the impact of users' CSE, CCA, and CS on CMI. The results of this study were expected to provide better understanding on cybersecurity gaps and threats in government agencies (Aakash, 2006; Besnard & Arief, 2004; Blanke, 2008; D'Arcy et al., 2009; Dinev et al., 2008; Rezgui & Marks, 2008; Torkzadeh & Lee, 2003; Veiga & Eloff, 2007).

Barriers and Issues

The main barrier of this study was that cybersecurity studies are not widely conducted in U.S. government agencies due to the government agencies' strict union rules, organizational politics, as well as managerial support and funding. The first issue of this study was that the participants were not willing to share information about their knowledge of cybersecurity skills due to their concerns about their privacy (Straub, 1986; Straub & Nance, 1990). In order to address the participants' concern, they were informed that their participation was voluntary. They were told that their survey responses would be anonymous to ensure confidentiality as well as privacy of each participant and that any data collected would be used for this study only. The second issue was that the number of participants was limited. The main reason for the limited sample size was because this cybersecurity survey was voluntary. Therefore, an explanation of the importance of their participation and the value of the results of the study to the organization were communicated to participants and senior management prior to the survey. In addition, the time collecting and analyzing the data was lengthy due to the need of a review of the survey questions by an expert panel before collecting data. Lastly, another issue in conducting this study was the need for institutional review board (IRB) approval. Given that the study involved human subjects, the instruments and protocols used had to be approved by the University's IRB prior to the study being conducted. IRB approval was obtained to conduct this research study.

Definition of Terms

Computer misuse intention (CMI) – An individual's intention to perform a behavior that is defined by the organization as a misuse of IS resources (D'Arcy et al., 2009).

Computer self-efficacy (CSE) – A judgment of one's capability to use a computer (Compeau & Higgins, 1995).

Cybersecurity – Prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems to ensure confidentiality, integrity, and availability (Axelrod, 2006).

Cybersecurity action skill (CAS) – The ability to commit to objectives, to meet security compliance (Levy, 2005).

Cybersecurity initiative skill (CIS) – The ability to seek out and take advantages of security software (e.g., antivirus program) and best practices (Levy, 2005).

Cybersecurity computing skill (CCS) – The ability to use protective tools (e.g., antivirus software) to protect computers and computer networks to secure data and information system (Levy, 2005).

Cyberspace – Independent network of IT infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries (The White House, 2009).

Cyberterrorism – Concerted, sophisticated attacks on networks (Foltz, 2004).

Cyberwar – Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption (Clarke & Knake, 2010).

Information Security - The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use (Rezgui & Marks, 2008).

Information System (IS) – The system that governs the information technology development, use, application, and influence on a business or corporation (Alvarez, 2002).

Information Technology (IT) –The acquisition, processing, storage, and dissemination of vocal, pictorial, textual, and numerical information by a microelectronics-based combination of computing and telecommunications (Caputo, 2010).

Negative Technologies – Tools used for breaking into systems and databases, such as computer viruses and spyware (Dinev & Hu, 2007).

Protective Technologies – Technologies that are designed to deter, neutralize, disable, or eliminate the negative technologies or their effectiveness, such as anti-virus software, anti-spyware, firewalls, and intrusion detection technologies (Dinev & Hu, 2007).

Risk – The potential that a given threat will exploit vulnerabilities of an asset or group of assets (Rezgui & Marks, 2008).

Risky End-User Computing Behavior – End-users sharing passwords, downloading unauthorized software, and opening emails from unknown sources (Aytes & Connolly, 2004).

Skill – A combination of ability, knowledge, and experience that enables a person to do something well (Boyatzis & Kolb, 1991).

Statistical Package for the Social Sciences® (SPSS) – A software tool utilized to perform data analysis.

Theory of Reasoned Action (TRA) – Theory that demonstrates the links between attitudes, beliefs, norms, intentions, and behaviors of individuals (Fishbein & Ajzen, 1975).

User – end-users or computer users are individuals who may develop their own applications or use codes written by others (Torkzadeh & Lee, 2003).

User awareness of computer monitoring (UAC-M) – The awareness by users of computer monitoring, which is tracking employees' Internet use, recording network activities, and performing security audits (D'Arcy et al., 2009).

User awareness of computer sanctions (UAC-S) – The punishment for breaking the cybersecurity rules set by the organization (D'Arcy et al., 2009).

User awareness of security policy (UAS-P) – The security policies with detailed guidelines for the proper and improper use of organizational IS resources (D'Arcy et al., 2009).

User awareness of security-training programs (UAS-T) – The programs that focus on providing users with knowledge of the information security policies and skills necessary to perform any required cybersecurity engagements (D'Arcy et al., 2009).

Web-based Survey – An online survey that has incorporated the functionality of the Internet (Thomas, 2003).

Summary

Chapter one provided an introduction to this study, identified the research problem, identified barriers to conducting this study, and provided an overall theoretical position. The research problem that this study addressed was the fast growing cybersecurity threats and vulnerabilities that are causing substantial financial losses on governments and organizations all over the world. The main focus was on the users' computer misuse intention (CMI) at government agencies. Valid literature supporting the research problem and the need for this study was presented.

This chapter also presented the main goal for this study, and specific goals. The main goal of this research study was to empirically test a predictive model on the impact of computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) on computer misuse intention (CMI) at government agencies. This research was built on previous studies conducted by D'Arcy et al. (2009), Levy (2005), Blanke (2008), Torkzadeh and Lee (2003), as well as Aakash (2006), by investigating the contributions of user's CSE, CCA, and CS toward CMI in an attempt to validate a model to assess user's CMI in a government agency. The first specific goal of this study was to empirically assess CSE and its contribution to CCA dimensions. The second goal of this study was to empirically assess CCA dimensions and its contribution to CS. The third goal of this study was to empirically assess CS and its contribution to CMI. The fourth goal of this study was to empirically assess if there is a significant difference on the measured constructs based on age, gender, job function (i.e., job title), education level, length of working in the organization, and military status (e.g., veteran). The last goal was to empirically assess the fit of the model by using CSE, CCA (i.e., UAS-P, UAS-T, & UAC-M), CS (i.e., CCS, CIS, & CAS), CMI, and control variables.

There were a total of four hypotheses. H1 tested the CSE influence on the CCA dimensions (i.e., UAS-P, UAS-T, & UAC-M). H2 (i.e., H2a, H2b, & H2c) tested the CCA influence on the CS dimensions (i.e., CCS, CIS, & CAS). H3 tested the CS influence on CMI. H4 (i.e., H4a, H4b, H4c, H4d, H4e, H4f, & H4g) tested for differences based on CSE, CCA, CS, and CMI demographics variables.

The relevance and significance of the study were also presented in this chapter. According to the literature, researchers are in agreement that more focus needs to be placed on the aspects of users' computer misuse intention (CMI), as this significantly influences the realization of a stronger cybersecurity (Blanke, 2008; D’Arcy et al., 2009; Dinev et al., 2008; Torkzadeh & Lee, 2003). The significance of this study was expected to be in the results of the assessment on the role of user CSE, CCA, and CS toward CMI at government agencies, as well as the investigation of the impact of user CSE, CCA, and CS on CMI. The results of this study provided better understanding on cybersecurity gaps and threats in government agencies (Aakash, 2006; Besnard & Arief, 2004; Blanke, 2008; D’Arcy et al., 2009; Dinev et al., 2008; Rezgui & Marks, 2008; Torkzadeh & Lee, 2003; Veiga & Eloff, 2007). The methods to address barriers and issues were discussed. The chapter ended with a definition of terms used throughout this study and any related acronyms.

Chapter 2

Review of the Literature

Introduction

The literature review was presented to provide the theoretical foundation for this study. Relevant computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA) (i.e., UAS-P, UAS-T, & UAC-M), and cybersecurity skills (CS) (i.e., CCS, CIS, & CAS) literature were reviewed as they play an important role in the user CMI in government agencies. As suggested by Hart (1998), the literature review will focus on "appropriate breadth and depth, rigor and consistency, clarity and brevity, and effective analysis and synthesis" (p. 1). Constructs are an important part of the literature review (Hart, 1998). In the following section, the constructs of this study are reviewed to provide an understanding of the constructs, identify prior research that is focused on these constructs, and discuss what is known about the constructs.

Computer Self-Efficacy

The construct of CSE proposed by Compeau and Higgins (1995) was based from the general concept of self-efficacy that was founded on social cognitive theory (Bandura, 1977, 1984). Self-efficacy is defined as "people's judgments of their capabilities to organize and execute courses of action required to attain designated performances" (Bandura, 1986, p. 391). CSE pertains to individuals' judgment of their capabilities to use computers in various situations (Marakas et al., 1998). Compeau and Higgins (1995) defined self-efficacy “as beliefs about one’s ability to perform a specific behavior” (p. 146). Compeau and Higgins (1995) specified that CSE is “an individual’s perception of his or her ability to use a computer in the accomplishment of a job task” (p. 193). Compeau and Higgins (1995) stated that individuals who are more confident in their computer skills are more likely to expect positive results in their computer use. Individuals’ judgment of their ability to complete a task using computers influences their decision on how they will use computers (Piccoli, Ahmad, & Ives, 2001). Research has shown that CSE applies a significant influence on an individual’s decision to use computers to achieve various tasks (Compeau & Higgins, 1995; Marakas et al., 1998). Literature suggests that CSE has a very high reliability and strong validity across different contexts (Levy & Green, 2009).

Compeau and Higgins’ (1995) study of 1,020 randomly selected management individuals found that CSE exerted “a significant influence on individuals’ expectations of the outcomes of using computers, their emotional reactions to computers (affect and anxiety) as well as their actual computer use” (p. 189). Compeau and Higgins (1995) concluded that computer users with higher CSE had higher usage of computers, enjoyed using them more, and possessed less computer related anxiety. According to D’Arcy (2006), in a study of 507 individuals that use computers at work, “those that feel more comfortable using computers can better comprehend the messages conveyed in security awareness programs and therefore become more convinced of the organization’s seriousness toward IT security” (p. 158). D’Arcy indicated based on research findings that “computer self-efficacy influenced the effectiveness of security countermeasures” (p.

175). Compeau, Higgins, and Huff (1999) claimed that studies have uncovered a close relationship between self-efficacy, skill, as well as individual reactions to technology usage and adoption. Levy and Green (2009) found that CSE had a positive influence on users' perceptions on ease of use and system usefulness. According to Levy and Green (2009), "sailors who are comfortable working with IS and learning to use them on their own, are more likely intended to use such systems" (p. 30).

Computer skill pertains to an individual's ability to utilize computer hardware and software to design, develop, modify, and maintain specific applications for task-related activities (Torkzadeh & Lee, 2003). Computer skills and computer self-efficacy are interrelated due to the nature that both are outcomes of development and transformation of the users' skill levels (Fischera, 1980; McCoy, 2010). For example, CSE is one's perceptions about his/her ability to detect and remove hidden-malware in his computer and skill is one's professed ability to detect and remove the hidden-malware in his/her computer. Torkzadeh, Chang, and Demirhan (2006) suggested that CCA "significantly improved computer and Internet self-efficacy" (p. 541). It appears that CSE plays an important role in influencing users' perception on CCA (Piccoli et al., 2001).

User Awareness of Security Policy

UAS-P pertains to security policies. D'Arcy et al. (2009) stated that "security policies contain detailed guidelines for the proper and improper use of organizational IS resources" (p. 80). Security policies are similar to societal laws because they provide information of what constitutes unacceptable conduct, which increases the user's perceived threat of punishment for illegal behavior (J. Lee & Lee, 2002). Straub's (1990) survey of 1,211 organizations found that users' awareness of security policies were associated with a lower level of users' computer abuse. When users are not motivated to follow or not aware of security policies designed to protect both users and organizations, security fails (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009).

D'Arcy et al. (2009) found that computer policy statements "prohibiting software piracy and warning of its legal consequences resulted in lower piracy intentions" (p. 81). The absence of security policies can lead to a misinterpretation of acceptable computer use by users (Straub, 1990). This can lead users to assume that computer misuse is not subject to enforcement and has little to no consequence (Straub, 1990). The effects of computer security policies on users' computer misuse intention suggest that users' awareness of the existence of security policies decreases the probability of engaging in computer misuse (Blanke, 2008; D'Arcy et al., 2009). But more research is needed to better assess the impacts of UAS-P on CMI.

User Awareness of Security-Training Programs

UAS-T pertains to security training programs. Security training programs focus on providing users with knowledge of the information security policies needed to perform any required cybersecurity activities (D'Arcy et al., 2009). D'Arcy et al. (2009) found that information security training programs could help reduce users' CMI. Information security training programs reinforce acceptable computer usage guidelines and emphasize the potential consequences for computer misuse (D'Arcy et al., 2009). One of the biggest causes of computer security failures is the lack of computer security training programs to develop users' cybersecurity awareness (Boss et al., 2009). Information security researchers have argued that information security training programs are essential in helping users understand the impact of computer misuse (Blanke, 2008; D'Arcy et al., 2009). It is important to evaluate the learners' tendency to actually apply what they have learned and the confidence they have developed in their ability (Piccoli et al., 2001).

An UAS-T program includes ongoing efforts to convey awareness to users about cybersecurity risks in the organizational environment, emphasizing recent actions against users that committed computer misuse and increasing users' awareness of their responsibilities regarding organizational information resources (D'Arcy et al., 2009; Straub & Welke, 1998). Straub and Welke (1998) stated that the primary reason for initiating UAS-T programs is to "convince potential abusers that the company is serious about security and will not take intentional breaches of this security lightly" (p. 445). UAS-T has a positive influence on user CS by providing information about acceptable and unacceptable usage of information systems, punishment associated with computer abuse, and awareness of organizational enforcement activities (Wybo & Straub, 1989). Wybo and Straub (1989) found that UAS-T has a positive effect on three cybersecurity skills (CCS, CIS, & CAS). However, additional research is required to better assess the contribution of UAS-T on CS.

User Awareness of Computer Monitoring

UAC-M is often used by organizations to gain compliance with rules and regulations (D'Arcy et al., 2009). D'Arcy et al. (2009) stated that "computer monitoring includes tracking employees' Internet use, recording network activities, and performing security audits" (p. 80). Computer monitoring of activities appears to deter user computer misuse because it increases the perceived chances of detection and punishment for such behavior (D’Arcy et al., 2009; Straub, 1990). Computer monitoring directly influences user computer misuse intention (D’Arcy & Hovav, 2009; Urbaczewski & Jessup, 2002).

Studies from criminology and sociology found that monitoring and surveillance help deter users’ computer misuse (Alm & McKee, 2006; D’Arcy et al., 2009). IS studies suggest that computing monitoring can reduce user computer misuse while increasing perceived certainty and severity of sanctions for computer misuse (D’Arcy et al., 2009; Straub & Nance, 1990). Monitoring user computing activities is an active security measure that enables organizations to detect and take appropriate actions on computer misuse (D’Arcy & Hovav, 2009; D’Arcy et al., 2009). It seems that appropriate monitoring practices increase an organization’s ability to prevent intentional computer misuse incidents that are likely to cause financial impact (D’Arcy et al., 2009). D’Arcy et al. (2009) indicated that UAC-M has negative influence on users’ computer misuse intentions (D’Arcy et al., 2009). Torkzadeh and Lee (2003) found that CS plays an important role towards CMI. Therefore, additional research is needed to better assess the impacts of UAC-M on CS.

User Awareness of Computer Sanctions

In the context of UAC-S, general deterrence theory (GDT) theorizes that the greater the certainty and severity of sanctions for banned acts the more users’ intention for committing such behavior is decreased (Gibbs, 1975). Sanction is the punishment for breaking the cybersecurity rules set by the organization (D’Arcy et al., 2009). D’Arcy et al. (2009) defined “certainty of sanctions as the probability of being punished” while "severity of sanctions refers to the degree of punishment" (p. 82) in the context of committing computer misuse. Researchers found that sanction fear helps to predict criminal and illegal behaviors (D'Arcy et al., 2009). For example, hacking and stealing intellectual property (e.g., program code) from organizations has more weight on sanction fear than sharing password among co-workers.

The effectiveness of UAC-S on perceptions of punishment severity appears to be important because perceived punishment severity is a deterrent to computer misuse (D'Arcy et al., 2009). Sanctions derive from the GDT. This theory suggests that perceived certainty, severity, and celerity of punishment affect people's decision on CMI (Pahnila, Siponen, & Mahmood, 2007). D'Arcy and Hovav (2009) suggested that the strength of sanctions influences users' ethical judgments and increases their perception of the negative consequences of committing computer misuse. D'Arcy et al. (2009) found that perceived severity of sanctions had a negative effect on user CMI, but perceived certainty of sanctions did not have a negative impact. Hovav and D'Arcy (2012) found that UAC-S may be significantly different across national cultures (e.g., U.S. vs. Korea). Sanctions have been found to have no significant effect on CMI. This relationship was well documented in literature as not supported (D'Arcy et al., 2009; Pahnila et al., 2007). Therefore, UAC-S was not measured as it is well documented to not have significant factor in the impact of UAC-S on CMI.

Skills

Skill is the ability to understand and make use of different intellectual abilities to achieve the most appropriate action for the best result (Levy, 2005; Torkzadeh & Lee, 2003). Boyatzis and Kolb (1991) defined skill as a “combination of ability, knowledge and experience that enables a person to do something well” (p. 280). The theory about skill provides predictable development sequences in any field by integrating behavioral and cognitive developmental concepts (Fischera, 1980; Udo, Bagchi, & Kirs, 2010). Cognitive development is the skill structure called developmental levels (Fischera, 1980). The transformation rules define the developmental levels by which a skill moves gradually up from one level to another; on each developmental sequence the individual controls a particular skill (Fischera, 1980). Skills are gradually transformed to produce continuous behavioral changes (Fischera, 1980; Udo et al., 2010). Skills influence people’s experience, attitude, and behavior (Udo et al., 2010). Skills increase a person’s efficiency and positive behavior (Pryor, Cormier, Bateman, Matzke, & Karen, 2010). Users’ skills can be developed and improved when they are aware and engaged in adequate CCA initiatives (Pryor et al., 2010). It appears that cybersecurity countermeasures awareness dimensions (UAS-P, UAS-T, & UAC-M) of users have a positive influence on the three cybersecurity skills (CCS, CIS, & CAS) (Fischera, 1980; Pryor et al., 2010; Udo et al., 2010). Torkzadeh and Lee (2003) found that cybersecurity skills (CCS, CIS, & CAS) play a significant role in CMI. Therefore, it can be concluded that additional research on CS is needed to better assess the impacts of CS on CMI.

Information Technology Skills

Torkzadeh and Lee (2003) claimed that the “effective use of information technology (IT) is considered a major determinant of economic growth, competitive advantage, productivity, and even personal competency” (p. 607). Benitez-Amado, Perez-

Arostegui, and Tamayo-Torres (2010) defined IT as the technological resources that include “hardware, software, databases, applications and networks” (p. 89). IT skills include the domains of management of information systems principles (Caputo 2010; Havelka & Merhout, 2009). IT skill is the knowledge and ability to use computer hardware, software, and procedures to develop specific computer applications (Torkzadeh & Lee, 2003). Furthermore, the knowledge of computer programming languages, use of databases, and computer programs such as antivirus programs are considered to be part of IT skills (Havelka & Merhout, 2009; Torkzadeh & Lee, 2003).

There are two types of IT skills: a) soft IT skills and b) hard IT skills (Swinarski, Parente, & Noce, 2010). The soft IT skills cover the IT business, IT project management, and IT team domains, while the hard IT skills cover the computer software, hardware, network, and security domains (Swinarski et al., 2010). IT skills for Information Systems (IS) professionals can be said to be technical, technology management, and interpersonal management skills (Havelka & Merhout, 2009). Havelka and Merhout (2009) developed an IT skills framework consisting of hardware, software, business knowledge, business, management, social, system knowledge, problem solving, and development methodology skills. Havelka and Merhout (2009)’s IT skills framework is an important foundation in the IT field. IT skills can be said to be the foundation of cybersecurity skills because users need an appropriate level of IT skills to effectively learn and utilize their cybersecurity skills (Havelka & Merhout, 2009; Lerouge, Newton, & Blanton, 2005).

Cybersecurity Skills

Cybersecurity skills (CS) correspond to the technical knowledge surrounding the hardware and software required to implement information security (Lerouge et al., 2005). According to Lerouge et al. (2005), information system users need an appropriate skill set to effectively utilize cybersecurity functions and innovations. In their case study, Ramim and Levy (2006) found that three of the main causes of system failure were due to users' limited technology knowledge and skill, users' computer abuse, as well as the lack of proper cybersecurity policies and procedures. Ramim and Levy (2006) claimed that the majority of cybersecurity attacks come from insiders (e.g., employees), but unfortunately most of the attention is given only to outsiders' (e.g., hackers) attacks.

One of the weakest and most difficult aspects of security governance is the user CS management that consists of user awareness, education and training, ethical conduct, trust, as well as privacy (Rezgui & Marks, 2008; Veiga & Eloff, 2007). The leading reason is because user cybersecurity management deals with humans (e.g., computer users). Besnard and Arief (2004) found that "humans obey least-effort rules because they are cognitive machines that attempt to cheaply reach flexible objectives rather than to act perfectly towards fixed targets" (p. 261). Having users enroll in cybersecurity training and making them comply with the security guidelines could be a daunting process. Users need to understand the importance of cybersecurity skills on both their personal and professional levels (Rezgui & Marks, 2008). Computer users would be more interested in taking the cybersecurity training if they knew the importance of CS to protect their home and organization's computers from cybersecurity threats (Rezgui & Marks, 2008).

Users play an important role in contributing to cybersecurity solutions (Straub, 1990; Straub & Welke, 1998). The vast majority of IT managers and leaders acknowledge that cybersecurity is important to the organization (Dinev & Hu, 2007; Ruighaver et al., 2007). However, they are reluctant to support and fund cybersecurity initiatives such as training due to the lack of understanding that cybersecurity is everyone's responsibility; most senior management tend to rely on protective technologies only (Dinev & Hu, 2007; Ruighaver et al., 2007). Users are often resistant to security policies and bypass them, thus exposing their organizations to data loss and cybercrime (Boss et al., 2009). It is worth noting that managers and employees also tend to think of cybersecurity as a second priority compared with their own efficiency or effectiveness matters because the latter have a direct and material impact on the outcome of their work (Besnard & Arief, 2004). Boss et al. (2009) found that "despite the prevalence of technical security measures, individual employees remain the key link – and frequently the weakest link – in corporate defenses" (p.151).

Rezgui and Marks (2008) argued that the incompetence of users who underestimate the dangers inherent in their actions represents one of the biggest computer security problems. They stated that CCA should help overcome the users' cybersecurity incompetence problem by helping them increase their cybersecurity skills. CCA is vital in developing users' CS (Fischera, 1980; McCoy, 2010). Developing users CS will change their cybersecurity behavior in positive ways (Boss et al., 2009; McCoy, 2010). In fact, cybersecurity objectives cannot be met by technical and procedural protection only. CS plays an important role in helping ensure effective users' cybersecurity awareness which can aid in discouraging CMI (Besnard & Arief, 2004; Rezgui & Marks, 2008). Therefore, more research is needed to better assess the impacts of CS on CMI.

Cybersecurity Computing Skill

Cybersecurity computing skills (CCS) correspond to the technical knowledge surrounding the hardware and software required to implement information security (Lerouge et al., 2005). CCS can be defined as the ability to use protective applications (e.g., antivirus software) to protect computers, computer networks, and information systems (Levy, 2005). According to Lerouge et al. (2005), information system users need appropriate CCS set to effectively utilize cybersecurity functions and innovations.

One of the main causes of information security failure is due to users' limited CCS (Ramim & Levy, 2006). Ramim and Levy (2006) stated that most of cybersecurity attacks and abuse are done by employees from within the organization (e.g., computer users), but most of the attention is given only to attacks and threats from outside. Hacking, negative technologies (e.g., viruses), and theft are not the only threats to information systems (Drevin et al., 2007). One of the biggest threats from users is human error and misuse of computer assets (Drevin et al., 2007). Increasing users' CCS can help reduce human error and misuse of computer assets (D'Arcy et al., 2009; Drevin et al., 2007). It appears that CCS has a negative influence on users' computer misuse intention (Drevin et al., 2007; Ramim & Levy, 2006). Thus, additional research on CCS is needed to better assess the impacts of CCS on CMI.

Cybersecurity Initiative Skill

Initiative is a psychological transition that helps transform individual work roles and responsibilities into desired outcomes (Rank, Pace, & Frese, 2004). Initiative skill is a capacity to direct attention and effort over time toward a challenging goal (Dworkin, Larson, & Hansen, 2003). Cybersecurity initiative skills (CIS) can be defined as the ability to seek out and take advantage of security software (e.g., antivirus programs) and best security practices (Levy, 2005). Activities such as cybersecurity training are experiences in which users develop CIS by learning about how to make plans, overcome obstacles, and achieve desired goals (Dworkin et al., 2003). Personal initiative is the combination of proactive, self-starting, persisting behaviors that workers perform to achieve their desired goals (Dreu & Nauta, 2009). A study of 300 individuals suggested that individuals who held high complexity roles and jobs showed more personal initiative (Dreu & Nauta, 2009).

It is unlikely for users to take any initiative toward cybersecurity if they don't perceive it as useful (Davis, 1989). Albrechtsen (2007) claimed that a "user-involving security awareness program approach is much more effective for influencing user awareness behavior than general security awareness campaigns" (p. 283). According to Cone, Irvine, Thompson, and Nguyen (2007), many organizations initiate a general security campaign with hopes to educate and train users in cybersecurity. For example, general security campaigns are sending emails or notes to the users or publishing in the organizations' Intranet Website information about security. Unfortunately, general security campaigns are vastly ignored by most users (Cone et al., 2007). According to Cone et al. (2007), many forms of cybersecurity awareness initiatives fail because they are simple routines that do not require users to take initiatives and apply security concepts. Therefore, a carefully designed CCA program appears to be vital in an attempt to increase users' CIS (Cone et al., 2007).

Technology savvy users don't automatically become cybersecurity savvy. In other words, users' CIS does not automatically increase with their knowledge of technology (Cronan, Foltz, & Jones, 2006). According to Cronan et al.'s (2006) study of 516 students, participants who were more familiar with computers committed significantly more computer abuse. Aytes and Connolly (2004) claimed that it is unlikely that users will significantly change their cybersecurity behavior by just being provided information regarding computing risk. User's CIS on ethical conduct, trust, risk, and privacy may positively impact users' CMI (Rezgui & Marks, 2008; Veiga & Eloff, 2007).

Cybersecurity Action Skill

Cybersecurity action skill (CAS) was defined as the ability to commit to objectives to meet security compliance (Levy, 2005). An action involves a collection of commitments that are applied to objectives (Fischera, 1980; Levy, 2005). Therefore, action must always be adapted to commitments (Fischera, 1980). For example, every time a user recognizes a familiar computer application, the action is adapted to the specific application (Fischera, 1980). Every time an action is carried out, even on the same objectives, it is usually done slightly differently (Fischera, 1980). Thus, the users can control the relevant action variations on objectives (Fischera, 1980). Action produces results, makes applications work, and causes events to occur (Korukonda, 1992). Thus, users' CAS is important for positive cybersecurity outcome (Korukonda, 1992).

Action theory provides a three dimensional framework (Baum, Frese, & Baron, 2007). The three dimensions of the framework are sequence, structure, and focus (Baum et al., 2007). Sequence reflects the path from goals to feedback, structure indicates the level of regulation of action or skill to a meta-cognitive heuristic, and focus ranges from task to self (Baum et al., 2007). Action theory leads to cognitive ability, which is fundamental for entrepreneurs and employees to be able to take appropriate action (Baum et al., 2007).

According to Fishbein and Ajzen (1975) people's behavior is determined by their behavioral intention to perform the action. The intention is determined by the person's attitudes and subjective norms towards the behavior. The Theory of Reasoned Action (TRA) developed by Fishbein and Ajzen (1975) is a model that finds its roots in the field of social psychology. Fishbein and Ajzen's (1975) TRA defined the links between attitudes, beliefs, norms, intentions, and behaviors of individuals; see Figure 2.

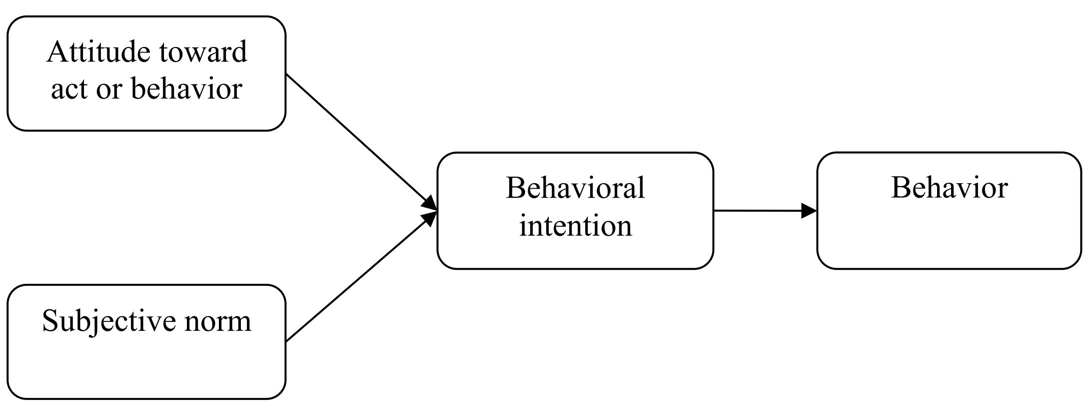

Figure 2. Theory of Reasoned Action (Fishbein & Ajzen, 1975)

The key focus of the Theory of Reasoned Action (TRA) is on the causal relationship between attitudes and behavioral intention; attitude influences behavioral intention which affects a person's behavior (S. Lee, Yoon, & Kim, 2008). According to

Fishbein (1980), reasoned action predicts that behavioral intent or action is caused by two main factors: attitudes and subjective norms. Similar to information integration theory, attitudes have two components. Fishbein and Ajzen (1975) called these the evaluation and strength of a belief. The second component influencing behavioral intent, subjective norms, also has two components. These components are normative beliefs (what one thinks others would want or expect him/her to do) and motivation to comply (how important is for one to do what he/she thinks others expect from him/her). Vallacher and Wegner (1987) suggested that “behavior dynamics are primary, with representations of action arising after the fact, or at best, concurrently with the action” (p. 3). Users’ attitude toward action or behavior influences intention, and intention is the main motivator of behavior (Fishbein & Ajzen, 1975). Therefore, TRA could be said to be the foundation of CAS (Fishbein, 1980; S. Lee et al., 2008). It appears that users’ attitude can be changed toward cybersecurity when CAS is increased (Fishbein, 1980; Korukonda, 1992). In addition, CAS can help decrease users’ CMI (Fishbein, 1980; Korukonda, 1992; Vallacher & Wegner 1987).

Many organizations use positive technologies to monitor users’ actions (e.g., browsing unsafe Internet sites) in the hopes of preventing them from wasting the company’s resources and downloading negative technologies (e.g., virus or worm) (Rezgui & Marks, 2008; Veiga & Eloff, 2007). It has been found that positive technologies don’t fully address all the cybersecurity risks since they can’t prevent users from engaging in risky activities (S. Lee et al., 2008; Rezgui & Marks, 2008; Veiga & Eloff, 2007). Numerous studies in psychology have been done on attitudes for predicting behavior and measuring the causal association between attitude and behavior (S. Lee et al., 2008). It appears that users' attitude and perceived social pressure, which is the predictor to behavioral intention, contribute to their actions (e.g., comply with security policies & procedures) (S. Lee et al., 2008). The main goal of implementing security policies and procedures is to secure the organizations' digital assets (Boss et al., 2009). Without an appropriate CCA program to educate the users' CAS, security policies and procedures can be meaningless (Boss et al., 2009). Ross (2006) suggested that CAS tends to keep users thinking and anticipating what if scenarios, thus preparing them to perform more adequately in an emergency without even thinking. CAS plays an important role on users' perception on CMI (Ross, 2006). Therefore, further research is needed to better assess the impacts of CAS on CMI.

Summary of What is Known and Unknown in Research Literature

The ability to learn a skill can be observed to be closely related to computer self-efficacy (Compeau & Higgins, 1995; McCoy, 2010). Skill is the ability to understand and make use of different intellectual abilities to achieve the most appropriate action for the best result (Levy, 2005; Torkzadeh & Lee, 2003). Thus, cybersecurity skill is the ability to understand and make use of different intellectual abilities such as using cybersecurity tools (e.g., data encryption) to protect the organization and personal sensitive computer data (Levy, 2005; Rezgui & Marks, 2008; Torkzadeh & Lee, 2003; Veiga & Eloff, 2007). Unfortunately, users are often resistant to security policies and bypass them, thus exposing their organizations to data loss and cybercrime (Boss et al., 2009). In addition managers and employees tend to think of cybersecurity as a second priority compared with their own efficiency or effectiveness matters, because the latter have a direct and material impact on the outcome of their work (Besnard & Arief, 2004). Cybersecurity countermeasures awareness tends to keep users thinking and anticipating what if scenarios, thus preparing them to apply the learned cybersecurity skills when required (Ross, 2006). Therefore, UAS-P, UAS-T, UAC-M, UAC-S, CCS, CIS, and CAS appear to play an important role on CMI (Besnard & Arief, 2004; D'Arcy et al., 2009; Rezgui & Marks, 2008).

It appears that CCA is inclusive to UAS-P, UAS-T, UAC-M, and UAC-S. UAS-P pertains to security policies, which are similar to societal laws, because they provide information on what constitutes unacceptable conduct, which increases the user's perceived threat of punishment for illegal behavior (D'Arcy et al., 2009; J. Lee & Lee 2002). UAS-T pertains to security training programs, which reinforce acceptable computer usage guidelines and emphasize the potential consequences for computer misuse (D'Arcy et al., 2009). UAC-M pertains to computer monitoring, which is often used by organizations to gain compliance with rules and regulations (D'Arcy et al., 2009). Computer monitoring directly influences user computer misuse intention (D'Arcy & Hovav, 2009). UAC-S pertains to computer sanctions, which is similar to prohibition of specific behaviors (e.g., computer misuse) (D'Arcy & Hovav, 2009). The impact of UAC-S on perceptions of punishment severity is important because perceived punishment severity is a strong deterrent to computer misuse (D'Arcy et al., 2009).

It seems that CS is inclusive to CCS, CIS, and CAS. CCS is the technical skill pertaining to the hardware and software knowledge that is required to implement proper cybersecurity (Lerouge et al., 2005). Information system users require an appropriate set of skills to employ cybersecurity technology functions more efficiently (Lerouge et al., 2005). CIS can be said to be the users' capacity to direct attention and effort over time toward a challenging goal such as implanting encryption to protect their sensitive data (Dworkin et al., 2003). CAS could be said to be the users' cybersecurity actions that produce positive cybersecurity results (Korukonda, 1992). Users that gain CCS, CIS, and CAS would be able to understand and implement cybersecurity technologies such as email encryption to secure their sensitive emails (Korukonda, 1992; Lerouge et al., 2005; Rank et al., 2004). Current literature appears to suggest that CSE, CCA, and CS can help reduce users' CMI (Korukonda, 1992; Lerouge et al., 2005; Rank et al., 2004); however, little attention has been given in research to provide empirical evidences for such interactions, while such validation in government organization appears to be highly needed.

Contributions of this Study

The main contribution of this study is to the improvement of current research in cybersecurity in the public sector by adding to the body of knowledge concerning government agencies' user CSE, CCA, CS and their impact on CMI. The results of this study also provide information that could influence or support future strategies aimed at cybersecurity practitioners and IT managers justify funding for cybersecurity programs for end users' cybersecurity awareness and skill development (Besnard & Arief, 2004; Blanke, 2008; D'Arcy et al., 2009; Dinev et al., 2008; Rezgui & Marks, 2008; Torkzadeh & Lee, 2003; Veiga & Eloff, 2007; White House, 2009). In addition, this study contributes to the research community by providing its findings for further research.

Another contribution of this study is that it helps to better understand various cybersecurity incidents that are generally caused by users. This research contributes to a better understanding of the causes of cybersecurity incidents attributable to users' CMI. Furthermore, this study contributes to more understanding of the necessary steps to help decrease users' CMI. Thus, the results of this study are in full agreement and supporting other IS literature that indicating that additional research is necessary to identify factors that influence individuals to engage in computer misuse activities (Blanke, 2008; D'Arcy et al., 2009; Dinev et al., 2008; Rezgui & Marks, 2008; Veiga & Eloff, 2007; White House, 2009).

Chapter 3

Methodology

Research Design

The main goal of this research study was to empirically test a predictive model on the impact of computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) on computer misuse intention (CMI) at government agencies. This study has assessed the role of users' CMI at a government agency. This field study used a Web-based survey instrument for data collection to test the relationships implied by Figure 1 and the research hypotheses put forth in Chapter 1. The survey was designed to capture respondents' perceptions of CSE, CCA, CS, and CMI. In this study, the participants were the computer users in a federal agency (Sekaran, 2003). Research design, sample, survey instrument and measures, validity and reliability, expert panel, pre-analysis data screening, as well as data analysis are presented in this chapter.

Survey Instrument and Measures

Researchers need to demonstrate that their developed instruments are measuring what they are designed to be measuring (Straub, 1989). According to Straub (1989), an "instrument valid in content is one that has drawn representative questions from a universal pool" (p. 150). Selecting the right survey wording that approximates the level of understanding of the participants is important (Sekaran, 2003). According to

Pinsonneault and Kraemer (1993), it is highly acceptable in research to collect data using surveys when independent and dependent constructs are well defined. Literature suggests that measures using a 7-point Likert scale appear to be more accurate than the 5-point Likert scale (D'Arcy et al., 2009; Levy & Green, 2009). Therefore, this study implemented a 7-point Likert scale following the scale established in literature for each of the measured constructs. This study used two different types of 7-point Likert scale to address different constructs. CSE, UAS-P, UAS-T, and UAC-M constructs were measured using 7-point Likert scale (1 = Strongly disagree to 7 = Strongly agree) in accordance to the validated constructs from literature (D'Arcy et al., 2009; Levy & Green, 2009) while CCS, CIS, and CAS constructs were measured with the 7-point Likert scale (1 = No skill or ability, 2 = I am now learning this skill, 3 = I can do this skill with some help from a supervisor, 4 = I am a competent performer in this area, 5 = I am an outstanding performer in this area, 6 = I am an exceptional performer in this area, and 7 = I am a leading performer in this area) in agreement with the validated constructs from literature pertaining to skill (Levy, 2005). According to Sekaran (2003), to ensure the content validity of the scales, the items selected must represent the concept about which generalizations are to be made. To check the validity of the survey, an expert panel was formed to include both academicians and practitioners. The expert panel reviewed the survey and provided recommendation(s) on wordings and clarity of the instrument.

The measure of the CSE construct in Appendix A was adapted from Levy and Green (2009) who studied the role of CSE in acceptance of the U.S. Navy's combat information system. The measures of the UAS-P, UAS-T, and UAC-M constructs in Appendix A were adapted from D'Arcy et al. (2009) who studied the role of user awareness of security countermeasures and its impact on information systems misuse. Lastly, the measures of CCS, CIS, and CAS constructs in Appendix A are based on Levy (2005)'s study on management skills comparison between online and on-campus Master of Business Administration (MBA) programs and Torkzadeh and Lee (2003)'s study that measured perceived user computing skills. The literature that serves as the foundation on which the survey questions are adapted from is detailed in Table 1.

Table 1. Survey question sources

Construct	No. of Items	No. of Items from Original Source	Original Scale Used	Survey Question Adapted From
Computer self-efficacy	3	3	7-point Likert scale	Levy & Green, 2009
User awareness of security policy	5	5	7-point Likert scale	D'Arcy et al., 2009
User awareness of security-training programs	5	5	7-point Likert scale	D'Arcy et al., 2009
User awareness of computer monitoring	6	6	7-point Likert scale	D'Arcy et al., 2009
Cybersecurity computing skill	6	12	5-point Likert scale	Torkzadeh & Lee, 2003
Cybersecurity initiative skill	6	6	7-point Likert scale	Levy, 2005
Cybersecurity action skill	6	6	7-point Likert scale	Levy, 2005
Computer misuse intentions	8	8	7-pint Likert	Hovav & D'Arcy, 2012

Validity and Reliability

External validity threats, such as addressing the interaction of selection and treatment, could be reduced when selecting groups with different racial, social, geographical, age, gender, or personality (Creswell, 2005). In this study, participants were from a government agency but were similar to the general user population. In order to provide representation of the general community, this study referenced to the data collected from the federal employees as detailed in Table 2 (United States Census Bureau, 2012).

Participants were well diversified (e.g., racial, social, geographical, age, gender, or personality) due to the nature of this government agency. The agency is located in the heart of a large metropolitan area in the northeastern U.S. and its employee's origin is from several different countries. It is almost impossible to find a group of participants to represent every aspect of individualities (e.g., personality, diversity, or culture). This study attempted to ensure that the study participants were closely representative of the general agency population by sending the survey to every computer user in the agency (Creswell, 2005).

Table 2. The summary of characteristics of federal employees (United States Census Bureau, 2012)

Federal Employees—Summary Characteristics: 1990 to 2008

[As of September 30. In percent, except as indicated. For civilian employees, excluding U.S. Postal Service employees]

Characteristics	1990	1995	2000	2003	2004	2005	2006	2007	2008
Average age (years) [1]	42.3	44.3	46.3	46.7	46.8	46.9	46.9	47.0	46.8
Average length of service (years)	13.4	15.5	17.1	16.8	16.6	16.4	16.3	16.1	15.5
Retirement eligible: [2]									
Civil Service Retirement System	8	10	17	27	30	33	37	41	46
Federal Employees Retirement System	3	5	11	12	13	13	13	13	13
Bachelor's degree or higher	35	39	41	41	42	43	43	45	44
Sex: Male	57	56	55	55	56	56	56	56	56
Female	43	44	45	45	44	44	44	44	44
Race and national origin:									
Total minorities	27.4	28.9	30.4	31.1	31.4	31.7	32.1	32.5	33.0
Black	16.7	16.8	17.1	17.0	17.0	17.0	17.2	17.3	17.5
Hispanic	5.4	5.9	6.6	7.1	7.3	7.4	7.5	7.6	7.7
Asian/Pacific Islander	3.5	4.2	4.5	4.8	5.0	5.1	5.1	5.4	5.2
American Indian/Alaska Native	1.8	2.0	2.2	2.1	2.1	2.1	2.1	2.1	2.1
Disabled	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0
Veterans preference	30.0	26.0	24.0	22.0	22.0	22.0	22.0	22.0	22.0
Vietnam era veterans	17.0	17.0	14.0	13.0	12.0	11.0	10.0	9.0	8.0
Retired military	4.9	4.2	3.9	4.6	4.9	5.4	5.7	6.0	6.3
Retired officers	0.5	0.5	0.5	0.8	0.9	1.0	1.1	1.2	1.3

[1] For full-time permanent employees. [2] Represents full-time permanent employees under the Civil Service Retirement System (excluding hires since January 1984), and the Federal Employees Retirement System (since January 1984).

Source: U.S. Office of Personnel Management, Office of Workforce Information, *The Fact Book, Federal Civilian Workforce Statistics*, annual. See also <http://www.opm.gov/feddata>.

Construct validity is the assessment of the translation of theories into actual measures or programs (Trochim, 2006). CSE construct is based on a well validated construct from Blanke (2008) that examined the contributions of CSE to the users' CMI. Blanke (2008)'s study was used as the groundwork to validate the impact of CSE toward CCA. UAS-P, UAS-T, and UAC-M constructs are based on a well validated construct from D'Arcy et al. (2009) who studied the role of users' awareness of security countermeasures and its impact on CMI. D'Arcy et al. (2009) provided the foundation to validate the influence of CAS on CS. CCS, CIS, and CAS constructs are based on the computing skill, initiative skill, and action skill that are validated constructs from Torkzadeh and Lee (2003)'s study that measured user computing skill, Levy (2005)'s study that measures skills in MBA programs, and Boyatzis and Kolb (1991)'s study on assessing individuality in learning skills. Their studies served as the groundwork to validate the impact of CS toward CMI. A social threat to construct validity exists, such as hypothesis guessing, evaluation apprehension, and experimenter expectation (Trochim, 2006). Since the survey instrument has been developed from five different sources (Blanke, 2008; Boyatzis & Kolb, 1991; D'Arcy et al., 2009; Levy, 2005; Torkzadeh & Lee, 2003), it was submitted to an expert panel for a thorough review and evaluation.

Expert Panel

The initial survey instrument was put through a review by an expert panel of cybersecurity professionals who evaluated the survey questions, the clarity of the questions, and the accuracy of the measurement instrument. The expert panel consisted of three prominent cybersecurity professors and five practitioners that intensely reviewed the survey instrument for validity. To ensure all scales were inputted in the same direction every survey question was reviewed prior to the data analysis (Levy, 2006). The expert panel members were asked to provide recommendations for modifications and essentially performed a thorough examination of the instrument's validity. The expert panel members were asked to (a) indicate their perception as to whether or not the individual items served to measure the constructs being evaluated, (b) recommend any additional items they believed could enhance the survey instrument, and (c) provide general comments on content and structure of the current survey instrument. The feedback from the expert panel was used to adjust the instrument as needed. In accordance with the approach of Straub (1989), adjustments included the removal of unnecessary items and the modification of questions, language, or layout of the instrument. The expert panel's feedback of the survey instrument was administered online over a couple of weeks using Google forms and surveys. Following the adjustments and testing, the finalized survey instrument that was used in this study was developed.

Sample and Data Collection

In this study, participants were invited from the local and state transportation agency, the largest among the nation's bridge and tunnel toll authorities in terms of traffic volume. The local and state transportation agency serves more than a million people daily in a large metropolitan area in the northeastern U.S. As a constituent agency of the local and state transportation agency, its dual role is to operate bridges and tunnels while providing surplus toll revenues to help support public transit.

This study targeted 500 participants with an anticipated response rate of 30%. According to Fowler (2009) the size of the sample has almost no impact on how well that sample is likely to describe the population. Fowler (2009) stated that “a sample of 150 people will describe a population of 15,000 or 15 million with virtually the same degree of accuracy” (p. 44). Demographic information such as age, gender, job function, education level, length of working in the organization, as well as military status such as veteran were collected. The demographic information can be used to describe the sample characteristics in the research to test the representation of the data collection to the generalized study population (Sekaran 2003).

Pre-analysis Data Screening

Pre-analysis data screening was performed before the data collection was analyzed in the Statistical Package for the Social Sciences® (SPSS). Pre-analysis data screening is important to ensure the accuracy of the collected data and to deal with the issues of response-set, missing data, and outliers (Levy, 2006). Accuracy of the collected data is critical since inaccurate data will result in invalid data analysis (Levy, 2006). Response-set is when a survey participant checks the same score for all the items. This can be addressed by eliminating the data from this participant from the final analysis (Blanke, 2008). Missing data can significantly impact the validity of the collected data (Blanke, 2008). To avoid missing data, the Web-based survey required all fields to be completed before submission. Lastly, Mahalanobis Distance was used to determine if any extreme cases, such as multivariate outliers existed and if the data should be included or eliminated from the data analysis (Blanke, 2008). According to Mertler and Vannetta (2001), an outlier can cause “a result to be insignificant when, without the outlier, it would have been significant” (p. 27). Thus, outlier cases were evaluated for removal prior to analyses. The survey was administered online over a few week period using Google forms.

Data Analysis

Carefully selecting the right process of data analysis is important (Creswell, 2005). This study used partial least square (PLS) to examine seven independent variables (CSE, UAS-P, UAS-T, UAC-M, CCS, CIS, & CAS) and their contributions on the dependent variable CMI. The PLS procedure has been gaining interest and use among IS researchers because of its ability to model latent constructs under conditions of non-normality and small to medium sample sizes (Compeau & Higgins, 1995). PLS is commonly recommended for predictive research models where the emphasis is on theory development (Chin, 1998). PLS employs a component based approach for estimation and has less restriction on sample size (Chin, 1998). PLS is suitable for analyzing complex models with latent variables (Chin, 1998). PLS is typically recommended in situations in which the sample size is small (Haenlein & Kaplan, 2004). Also, PLS was used to examine the contributions of the six control variables (i.e., age, gender, job function, education level, length of working in the organization, & military status such as veteran) on the dependent variable, CMI.

This study has evaluated the major hypothesis on CSE, UAS-P, UAS-T, UAC-M, UAS-S, CCS, CIS, CAS and CMI. Hypothesis 1, CSE of users will show significant positive influence on the cybersecurity countermeasures awareness dimensions (UAS-P, UAS-T, & UAC-M). Hypothesis 2 (a, b, c, d), Cybersecurity countermeasures awareness dimensions (UAS-P, UAS-T, & UAC-M) of users will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS). Hypothesis 3, the three cybersecurity skills (CCS, CIS, & CAS) of users will show significant negative influence on Computer Misuse Intention (CMI). Finally, Hypothesis 4 (a, b, c, d, e, f, & g), the six control variables (i.e., age, gender, job function, education level, length of working in the organization, as well as military status such as veteran) will show no significant influence on CMI. PLS was used to test the convergent and discriminant validity of the scales. In a confirmatory factor analysis (CFA) by PLS, convergent validity will be demonstrated when a measurement is loaded highly, its coefficient is above 0.60 or loaded significantly on the main factor, its *t* values are within the 0.05 level of their assigned construct (Gefen & Straub, 2005). In order to assess the reliability of the measurement items, the composite construct reliability coefficient was computed.

Model Fit

IBM SPSS® and SmartPLS® statistical packages were used to perform the model fit testing based on Partial Least Square (PLS). According to Haenlein and Kaplan (2004), PLS should be an appropriate technique for model fit examination. The four hypotheses were tested using a model-fit analysis. Wetzels, Odekerken-Schröder, and Van-Oppen (2009) suggested a global fit measure (GoF) for PLS path modeling as a geometric mean of the average communality and average R^2. They also indicated three cut-off points for GoF which are GoF(small) = 0.1, GoF(medium) = 0.25, and GoF(large) = 0.36. As such, the GoF for the model was calculated by PLS in the means of the average communality and average R^2.

Summary

This chapter provided an overview of the methodology that has been utilized to conduct this study. The population is described as working professionals at a government agency in the northeastern U.S. This chapter described the study that attempted to assess the role of user CSE, CCA, and CS as well as a set of six demographic variables toward CMI. A survey instrument was proposed based on validated prior measures. The study targeted 500 participants with an anticipated response rate of 30%. Data collection was outlined via the use of a Web-based survey instrument. The pre-analysis screening was performed before the data was collected (Levy, 2006). The collected data was analyzed in SPSS and PLS, while the GoF cut-of-points were proposed based on prior literature.

Chapter 4

Results

Overview

This chapter details the data analysis and the results of this study. The chapter is organized in a similar way to chapter three and, as such, will include an analysis of the data collection process and the statistical methods used to analyze the data, and the overall results. First, the quantitative phase will be presented, which details the results of this study. This will be followed by the results of the pre-analysis data screening and then the results of the quantitative phase. The chapter will conclude with a summary of the results and the procedures used for the analysis.

The main goal of this research study was to empirically test a predictive model measuring the impact of computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) on computer misuse intention (CMI) at government agencies, along with testing of a set of six control variables. The four specific research hypotheses addressed were:

H1: Computer self-efficacy (CSE) of users will show significant positive influence on the cybersecurity countermeasures awareness dimensions (UAS-P, UAS-T, & UAC-M).

H2a: User awareness of security policy (UAS-P) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H2b: User awareness of security-training programs (UAS-T) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H2c: User awareness of computer monitoring (UAC-M) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H3: The three cybersecurity skills (CCS, CIS, & CAS) of users will show significant negative influence on Computer Misuse Intention (CMI).

H4a: Users' *age* will show no significant influence on Computer Misuse Intention (CMI).

H4b: Users' *gender* will show no significant influence on Computer Misuse Intention (CMI).

H4c: Users' *job function* will show no significant influence on Computer Misuse Intention (CMI).

H4d: Users' *education level* will show no significant influence on Computer Misuse Intention (CMI).

H4e: Users' *length of working in the organization* will show no significant influence on Computer Misuse Intention (CMI).

H4f: Users' *military veteran status (i.e. 'yes' or 'no')* will show no significant influence on Computer Misuse Intention (CMI).

Pre-Analysis Data Screening

There were 185 responses received from the survey respondents. Before the collected data could be analyzed, pre-analysis data screening had to be performed. Pre-analysis data screening was performed to detect irregularities or problems with the collected data. According to Levy (2006), pre-analysis data screening is performed to ensure the accuracy of the data collected, to deal with the issue of response set, to deal with missing data, and to deal with extreme cases or outliers. For this study, data accuracy was not an issue as the Web-based survey instrument was designed to allow only a single valid answer for each question. Additionally, data collected did not require any manual input as it was submitted directly into an online spreadsheet that then, was downloaded directly for the analyses. The issue of missing data was also not an issue for this study as the Web-based survey instrument was designed to prevent final submission until all items were completed. To address the issue of response-sets, a visual inspection of all responses was performed to identify cases that had the same response to all of the questions. Response-set bias is a factor that produces a particular pattern of responses that may not correctly correspond to the true state of affairs (Mangione, 1995). Kerlinger and Lee (2000) recommended the analysis of data for potential response-sets, and that researchers consider the elimination of any such sets from the research prior to data analysis. No response-set cases were found in the collected data.

One of the main reasons for pre-analysis data screening was to deal with extreme cases (e.g., outliers). Stevens (2007) stated that an outlier is a data point that is usually very different from the rest of the data. In order to address multivariate extreme case(s), Mahalanobis Distance analysis was performed. There was one case (case # 115) identified using Mahalanobis Distance as a significant multivariate outlier. Therefore, case number 115 has been reviewed and removed from the analysis. Table 3 details the cases with multivariate extreme values that resulted from the Mahalanobis Distance analysis.

Table 3. Mahalanobis distance extreme values (N=184)

			Case Number	CaseID	Value
Mahalanobis Distance	Highest	1	115	115	113.93522
		2	100	100	93.35203
		3	70	70	89.36936
		4	2	2	87.16059
		5	7	7	84.32366
	Lowest	1	93	93	7.99108
		2	8	8	14.58894
		3	153	153	15.13792
		4	59	59	15.17484
		5	29	29	15.21067

Demographic Analysis

After completion of the pre-analysis data screening, 184 responses remained for analysis of which 48 or 26.1% were completed by females and 136 or 73.9% were completed by males. Analysis of the respondents' age indicated that 11 or 6% were 20 to 29 years of age, 28 or 15.2 % of respondents were between the ages of 30 to 39, 70 or 38% of respondents were between the ages of 40 to 49, 54 or 29.3% of respondents were between the ages of 50 to 59, and 21 or 11.4% of respondents were 60 and over. 27 or 14.7% of respondents were administrator staff, 67 or 36.4% were managerial, 33 or 17.9% were officers, 23 or 12.5% were people working in operations, three or 1.6% were security operators, 18 or 9.8% were IT people, 11 or 6% were professional staff, and the remaining two or 1.1% were others (e.g., College interns). Among the respondents, two or 1.1% were with the organization under one year, 24 or 13% were with the organization between 1- to 5-years, 35 or 19% were with the organization between 6- to 10 years, 52 or 28.3% were with the organization between 11 to 15 years, 23 or 12.5% were with the organization between 16 to 20 years, 31 or 16.8% were with the organization between 21 to 25 years, 4 or 2.2% were with the organization between 26 to 30 years, and 13 or 7.1% were with the organization for over 30 years. Approximately 50% (90 or 48%) had bachelor's degree. Also, 35 or 19% were veterans. Details on the demographics of the population are presented in Table 4.

Table 4. Descriptive statistics of population (N=184)

Item	Frequency	Percentage (%)
Gender		
Female	48.0	26.1
Male	136.0	73.9
Age		
Under 20	0.0	0.0
20-29	11.0	6.0
30-39	28.0	15.2
40-49	70.0	38.0
50-59	54.0	29.3
60 and over	21.0	11.4
Job function		
Administrative staff	27.0	14.7
Managerial	67.0	36.4
Officer	33.0	17.9
Operations	23.0	12.5
Security operator	3.0	1.6
Technical	18.0	9.8
Professional staff	11.0	6.0
Other:	2.0	1.1
Year(s) with current organization		
Under 1 year	2.0	1.1
1-5 years	24.0	13.0
6-10 years	35.0	19.0
11-15 years	52.0	28.3
16-20 years	23.0	12.5
21-25 years	31.0	16.8
26-30 years	4.0	2.2
over 30 years	13.0	7.1
Education Level		
High School Diploma	36.0	19.6
2-years college (AA degree)	22.0	12.0
4-years college/university (Bachelor's degree)	90.0	48.9

Graduate (Master's degree)	29.0	15.8
Doctorate degree	1.0	0.5
Other:	6.0	3.3
Veterans		
Yes	35.0	19.0
No	149.0	81.0

Validity and Reliability Analyses

Model evaluation involves estimation of internal consistency, convergent discriminant validity tests to achieve construct validity, as well as reliability (Chin & Todd, 1995). Construct reliability is calculated by Cronbach's Alpha and composite reliability (Fornell & Lacker, 1981). The Cronbach's Alpha coefficients for all constructs in this study were greater than the threshold of 0.7 indicating very strong reliability for the constructs measured. The composite reliability implicitly assumes that each indicator has the same weight and it relies on actual factor loadings, which can be considered as the best measure for internal consistency (Fornell & Lacker, 1981). The composite reliability should be greater than 0.7 to reflect internal consistency. According to Table 5, all multi-item constructs measured have demonstrated very high composite reliability coefficients that are greater than 0.7, further validates the high reliability of all constructs measured. Convergence validity was assessed using average variance extracted (AVE). Fornell and Lacker (1981) suggested that greater than 0.5 is standard. All AVE were above 0.5 with exception of CMI being 0.434. AVE can be used to evaluate the discriminant validity. The value obtained from each construct should be greater than the variance divided between that construct and other variables in the model (Chin, 1998; Fornell & Lacker, 1981). Discriminant validity can be obtained by observing whether correlations between variables are less than the square of average variance extracted.

Table 6 shows that the squared value of average variance extracted for each construct is larger than the correlations in the same column (Chin, 1998; Fornell & Lacker, 1981).

Table 5. Descriptive statistics of reliability (N=184)

	AVE	Composite Reliability	R Square	Cronbach's Alpha
CAS	0.628582	0.910061	0.048279	0.883481
CCS	0.775289	0.953893	0.172877	0.941955
CIS	0.760665	0.950145	0.014402	0.939950
CMI	0.434217	0.858796	0.296575	0.818835
CSE	0.670791	0.858880		0.767531
UAC-M	0.608034	0.899040		0.871109
UAS-P	0.587071	0.875146		0.824381
UAS-T	0.667373	0.909265		0.875880

Table 6. Latent and Demographic Variables Correlation (N=184)

	Age	CAS	CCS	CIS	CMI	CSE	Education	Gender	Job Function	UAC-M	UAS-P	UAS-T	Veteran	Work Length
Age	1.000000													
CAS	-0.267780	1.000000												
CCS	-0.334663	0.647108	1.000000											
CIS	-0.271096	0.788711	0.760574	1.000000										
CMI	-0.153366	-0.216302	-0.009396	-0.174267	1.000000									
CSE	-0.308278	0.245487	0.380174	0.328085	-0.057794	1.000000								
Education	-0.044486	0.012302	0.034414	0.044656	-0.115584	0.252297	1.000000							
Gender	0.166827	0.261846	0.175785	0.224065	-0.115062	0.041387	-0.105108	1.000000						
Job Function	-0.226657	0.176227	0.317213	0.271661	0.127071	0.098225	0.018194	0.166158	1.000000					
UAC-M	0.023691	0.030543	-0.096926	-0.055363	-0.359816	0.063805	0.068386	0.049682	-0.138169	1.000000				
UAS-P	0.190391	0.219870	0.052369	0.120089	-0.354072	0.002130	-0.082055	0.161290	-0.168351	0.438059	1.000000			
UAS-T	0.158792	0.137169	-0.006738	0.055112	-0.399283	0.068480	0.007939	0.095754	-0.238748	0.533837	0.597236	1.000000		
Veteran	-0.056662	0.094477	0.103435	0.132019	-0.173653	0.110459	0.258886	-0.067184	-0.084258	0.140567	-0.003646	0.061502	1.000000	
Work Length	0.706256	-0.256021	-0.397878	-0.281894	-0.111722	-0.256803	-0.153081	0.034237	-0.262404	0.149427	0.200119	0.189568	-0.046002	1.000000

T-value has been obtained by running bootstrapping in SmartPLS. Given the data obtained, some adjustments in the proposed model path testing had to be taken into consideration for the model testing to reflect a viable model, which is slightly different than the one originally proposed. However, majority of the model path proposed were included in the tested model. T-value is used to identify the significance level of each path in the model. Based on this study with 184 degrees of freedom (df), T-values greater than 1.960 are significant at a p-value less than 0.05, T-values greater than 2.576 are significant at a p-value less than 0.01, and T-values greater than 3.291 are significant at a p-value less than 0.001 (Gravetter & Wallnau, 2009). Table 7 shows the coefficient and T-value of each set of constructs path. A correlation coefficient is a number between -1 and 1, which measures the degree to which two variables are linearly related. If there is a perfect linear relationship with positive slope between the two variables, then it is a correlation coefficient of 1; if there is positive correlation, whenever one variable has a high (low) value, so does the other. If there is a perfect linear relationship with negative slope between the two variables, then it is a correlation coefficient of -1; if there is negative correlation, whenever one variable has a high (low) value; the other has a low (high) value. A correlation coefficient of 1 means that the two numbers are perfectly correlated while a correlation coefficient of -1 means that the numbers are perfectly inversely correlated. A correlation coefficient of zero means that there is no linear relationship between the variables (Chin & Todd, 1995; Fornell & Larcker, 1981).

Table 7. Path coefficients significance (N=184)

Path	Coefficients	T Statistics	Significant
CAS -> CMI	-0.152762	1.118844	p = 0.265 Not supported

CCS -> CMI	0.243329	1.952593	p = 0.052 Limited support
CIS -> CMI	***-0.230363***	***1.973962****	p = 0.0499 Yes ($p < 0.05$)
CSE -> CCS	***0.391288***	***7.361295*****	Yes ($p < 0.001$)
CSE -> CMI	-0.019187	0.212218	p = 0.832 Not supported
UAC-M -> CCS	***-0.178643***	***1.991473****	p = 0.048 Yes ($p < 0.05$)
UAC-M -> CMI	***-0.190342***	***2.220108****	p = 0.028 Yes ($p < 0.05$)
UAS-P -> CAS	***0.219725***	***2.508762****	p = 0.013 Yes ($p < 0.05$)
UAS-P -> CCS	0.129809	1.625293	p = 0.106 Not supported
UAS-P -> CIS	0.120009	1.663104	p = 0.098 Not supported
UAS-P -> CMI	-0.104848	0.808814	p = 0.420 Not supported
UAS-T -> CMI	-0.166317	1.621924	p = 0.107 Not supported
Age -> CMI	-0.186975	1.719205	p = 0.087 Limited support H4a – rejected “age” has limited statistically significant negative impact on CMI
Gender -> CMI	-0.022814	0.262552	p = 0.793 Not rejected. As hypothesized “gender” has statistically no significant negative impact on CMI
Job Function -> CMI	0.041865	0.491383	p = 0.624 Not rejected. As hypothesized “Job Function” has statistically no significant negative impact on CMI
Education -> CMI	-0.071088	0.926183	p = 0.356 Not rejected. As hypothesized “Education” has statistically no significant negative impact on CMI
Work Length -> CMI	0.070697	0.723555	p = 0.470 Not rejected. As hypothesized “Work Length” has statistically no significant negative impact on CMI
Veteran -> CMI	-0.094907	1.274678	p = 0.204 Not rejected. As hypothesized “Veteran” has statistically no significant negative

			impact on CMI

*p<.05 (two-tailed tests).
**p<.001 (two-tailed tests).

PLS was used to address the four hypotheses. Results of the standardized PLS path coefficients model for this study is presented in Figure 3. The numbers noted on the arrows in the model represent the rounded path coefficient to the nearest hundredths value, where results indicated that five out of the construct 12 path coefficients (not including the demographic indicators) (CIS → CMI, CSE → CSS, UAC-M → CCS, UAC-M → CMI, & UAS-P → CAS) were significant at least at the p value of .05 level or greater (p<.001). The rest of the model paths (CSS → CMI, CAS → CMI, CSE → CMI, UAS-P → CCS, UAS-P → CIS, UAS-P → CMI, UAS-T → CMI, Age → CMI, Gender → CMI, Job Function → CMI, Education → CMI, Work Length → CMI, & Veteran Status → CMI) that were tested indicated path coefficients with non-significant p-values. Results of the R-squared (R^2) values are indicated below the given constructs where R^2 is applicable. R-squared (R^2) on CMI is 0.296 or nearly 0.30, an indicated acceptable model fit.

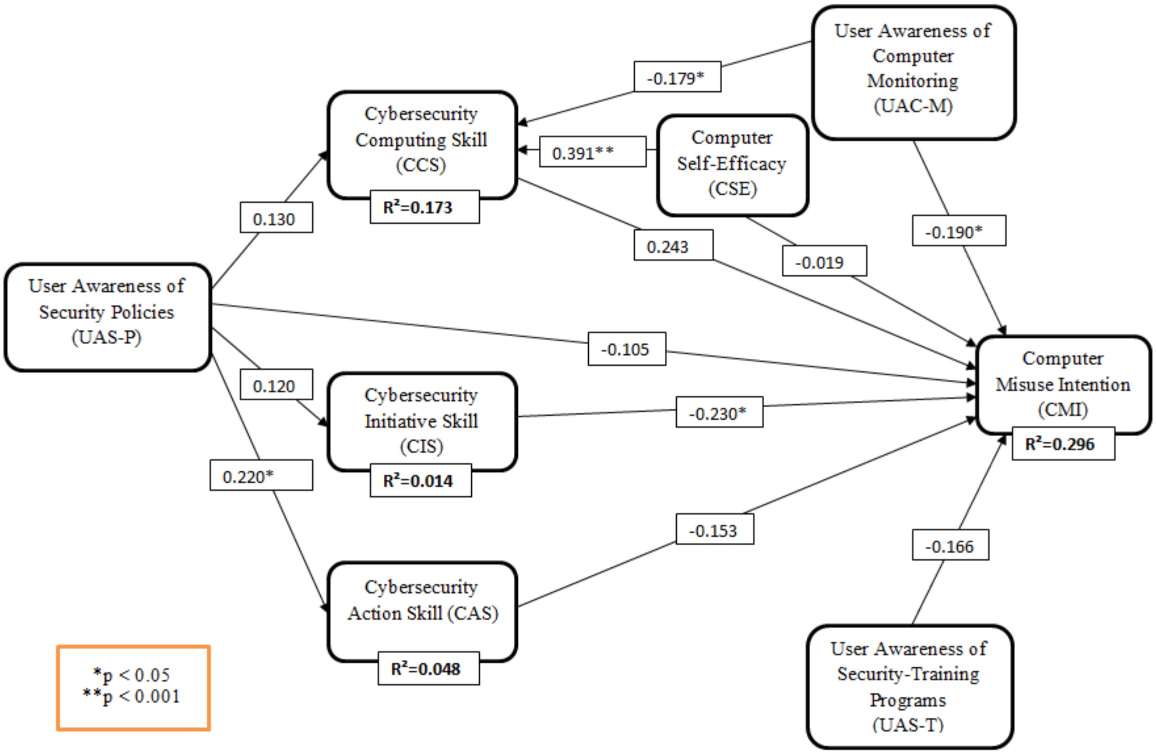

Figure 3. Results of the PLS analysis (N=184)

The results of the PLS model showed that UAC-M and CIS were significant contributors ($p < .05$) to CMI. UAC-M was also found to be a significant contributor ($p < .05$) to CCS. UAS-P was found to be a significant contributor ($p < .05$) to CAS. CSE made a significant contribution ($p < .001$) to CCS while it did not show significant contribution to CMI.

While this study found that CSE had no influence on CMI, which appears to be in support by prior research by D'Arcy and Hovav (2009) who found that CSE had also no effect on misuse intention. However, it might be that the relationship between CSE and CMI is just not linear. That is, those users with very low CSE are likely to engage in misuse unintentionally or out of ignorance, while users with very high CSE are likely to engage in misuse because they believe they can circumvent the system successfully and get away with it. As such additional research should be done on assessing such potential hyperbolic relations between the two constructs of CSE and CMI.

The mean scores of the CMI and CSE were obtained for the 184 records (see Figure 4). The findings show that by-in-large, only seven cases out of the total of 184 cases were CMI high, meaning that the majority (nearly 97%) of the respondents where ethical as their CMI was low. The most important finding is that majority (nearly 93%) of the participants had a high CSE while at the same time had a low CMI. This makes evident that there is a strong association between high CSE and low CMI. This suggests that, by-in-large, users with higher CSE have lower CMI, while such relationship may not be linear in nature and therefore, the low coefficient and T-value (i.e. high p-value) observed in this study. Phelps (2005) found that users with higher CSE were more effective at implementing system security. Crossler and Belanger (2006) stated that a user's level of CSE directly impacted his or her use of security tools. The plotting of the taxonomy of the mean scores of CMI and CSE as a 2x2 matrix summary is presented in Table 8. This study considered CSE and CMI < 4 to be note as "Low" and 4 > to be "High".

Table 8. CMI mean and CSE mean (N=184)

Item	Cases
CSE (low) and CMI (low)	7
CSE (high) and CMI (low)	170
CSE (low) and CMI (high)	0
CSE (high) and CMI (high)	7

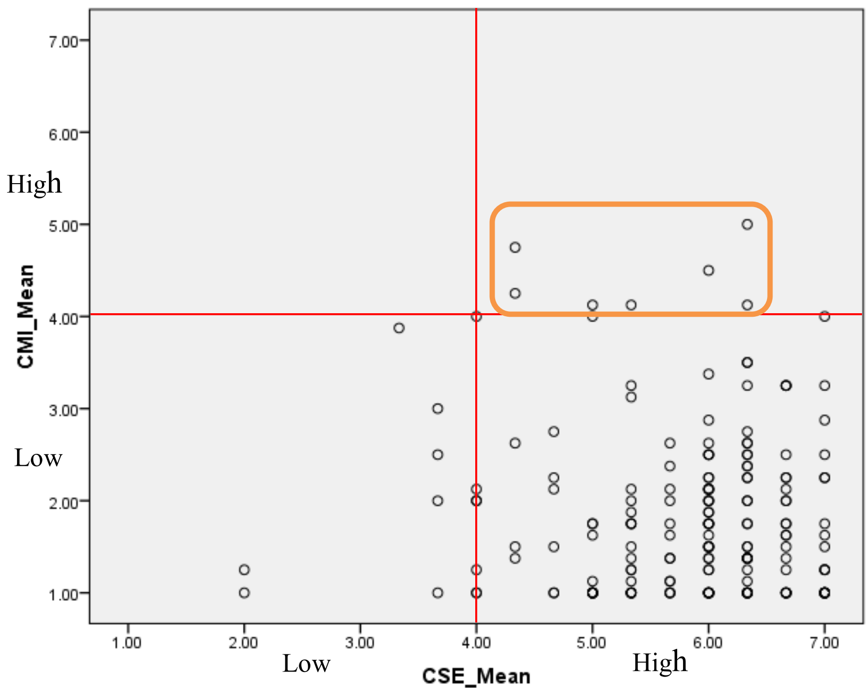

Figure 4. Graph of CMI mean and CSE mean (N=184)

Similar to the CSE to CMI path that suggested the case of the few high-CSE and high-CMI computer savvy users (e.g., users with high CCS), they feel that they can overcome the computer monitoring capabilities of their organizations and that they are less likely to be caught when engaging in computer misuse. Perhaps users with high CCS (e.g., hackers) might be more likely to engage in misuse because they believe they can circumvent the system successfully and get away with it. Therefore, someone with higher CCS could also appear to have higher CMI.

Summary

Chapter 4 reported on the results of all data analysis performed in order to answer the four hypotheses set in this study. In this chapter, the results of the contribution of CSE, CCA, and CS to CMI, as measured by the weight of their contribution to the prediction of CMI, are presented. Prior to the statistical analyses, pre-analysis data screening was performed to ensure the accuracy of the data collected. Following this screening, Cronbach's Alpha reliability tests were conducted for each construct to determine how well the items for each scale were internally consistent with one another. The results demonstrated high reliability for all constructs measured. In order to determine the representativeness of the sample, demographic data were requested from the survey participants. The distribution of the data collected appeared to be representative of the population of government employees.

PLS was used to address the four hypotheses and test the model fit. Given the type of data collected and the amount of constructs measured, modifications were needed from the original model proposed in order to test the path coefficients among the constructs measured. The results of the PLS model showed that UAC-M and CIS were significant contributors ($p <.05$) to CMI. UAC-M was also found as a significant contributor ($p <.05$) to CCS. UAS-P was found as a significant contributor ($p <.05$) to CAS. CSE demonstrated the most significant contribution ($p < .001$) to CCS while it didn't show significant contribution to CMI.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

This chapter begins with conclusions drawn from the results of this study. The main goal and hypotheses investigated are detailed next, and the implications of the study are discussed. Moreover, contributions of this study to the body of knowledge are presented followed by the limitations of this study. The chapter ends with recommendations for future research and a summary of this study.

The main goal of this research study was to empirically test a predictive model on the impact of computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) on computer misuse intention (CMI) at government agencies along with a set of six demographic indicators. The population of this study was working professionals from a government agency located in northeastern U.S. The original projected response rate was seeking 30% out of 500 potential participants, while the actual survey response rate obtained was nearly 37%, 184 usable records.

The first specific goal of this study was to empirically assess CSE and its contribution to CCA (UAS-P, UAS-T, & UAS-M) dimensions. The results of the PLS model indicated that CSE did not make any significant contribution to CCA. While not originally hypothesized, CSE demonstrated a significant contribution ($p < .001$) to CCS.

The second goal of this study was to empirically assess CCA (UAS-P, UAS-T, & UAS-M) dimensions and its contribution to CS (CCS, CIS, & CAS). Based on the PLS model, UAS-P demonstrated a significant contribution ($p < .05$) to CAS. UAC-M was found to be a significant contributor ($p < .05$) to CCS. Interestingly, UAS-T did not make any significant contribution to any of the CS dimensions.

The third goal of this study was to empirically assess CS (CCS, CIS, & CAS) and its contribution to CMI. The PLS model revealed that UAC-M and CIS were found to be significant contributors ($p < .05$) to CMI. CCS was found to demonstrate limited significant contribution ($p = 0.052$) to CMI.

The fourth goal of this study was to empirically assess to empirically assess age, gender, job function (i.e., job title), education level, length of working in the organization, and military status (e.g., veteran) and their contributions to CMI. The PLS model showed that most of the demographic latent variables didn't show any significance except for age, which showed limited significant difference ($p = 0.087$) to CMI.

The last goal was to empirically assess the fit of the model by using CSE, CCA (i.e., UAS-P, UAS-T, & UAC-M), CS (i.e., CCS, CIS, & CAS), CMI, and control variables. The PLS model presented the results of the study (see Figure 3). The results indicated that UAC-M and CIS made significant contributions ($p < .05$) to CMI. UAC-M showed significant contribution ($p < .05$) to CCS. UAS-P indicated significant contribution ($p < .05$) to CAS. Lastly, CSE demonstrated a significant contribution ($p < .001$) to CCS while it did not show significant contribution to CMI.

The purpose of our study was to assess the role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuse intention at government agencies. The results showed that UAS-P demonstrated a significant contribution to CAS and UAC-M demonstrated a significant contributor to CCS. This finding is consistent with the recommendations of IS security advocates who contend that security countermeasures awareness are important when it comes to cybersecurity skills. One area that did not demonstrate significant contribution from CCA was CIS. This suggests that, in the context of the data collected in this study, CCA increases users' CCS and CAS while it doesn't have a significant contribution on users' CIS. However, additional research maybe needed to further investigate these findings.

CSE showed significant contribution to CCS while it did not show significant contribution to CMI. The results suggest that while the CSE to CCS path is in accordance with the recommendations of IS security advocates who contend that computer self-efficacy by employees are valid to enhance as they also significantly measure their security countermeasures awareness. The non-significant result found in this study of CSE to CMI path suggests that in the case of the few high-CSE and high-CMI computer savvy users, they feel that they can overcome the computer monitoring capabilities of their organizations and that they are less likely to be caught when engaging in computer misuse. Computer savvy users may also know that security personnel cannot actively monitor all computing activities, even though such activities might get automatically logged and recorded by monitoring technologies. While these issues appear to be valid for the high-CSE and high-CMI computer users, the results indicated that 96% of the participants demonstrated, by-in-large, to be ethical with varied CSE, but a low CMI.

UAC-M and CIS were significant contributors to CMI. This is consistent with the recommendations of IS security advocates and researchers. CCS showed limited significant contribution ($p = 0.052$) to CMI. Contrary to expectations, UAS-T did not make any significant contribution to any of the CS dimensions or CMI. This finding was surprising since literature suggested that UAS-T should have a significant contribution to CS dimensions. One possible explanation for these results could be the relatively high age of the survey participants. In this study, majority of the participants were in the 40 years old and older age group, representing 78.7% of the participants. In addition, age was the only control variable that demonstrated limited significant contribution ($p = 0.087$) to CMI. As such, the impact of UAS-T on CS and CMI should be further investigated with different professional computer users to investigate if such results are specific for the data collected in this study or indeed due to the age issue.

Study Implications

This research study has a number of implications for the existing body of knowledge in the areas of IS and cybersecurity within government agencies. A prediction model was developed with CSE, CCA, and CS in an attempt to validate a model to predict employees' CMI in a government agency. These independent variables were selected for the model based on the literature search that was conducted. There are two key contributions that this study makes to IS and cybersecurity research. The first one is to develop and empirically validate a model for predicting government employees' CMI. While significant number of information security studies have been conducted using college students as participants, the second key contribution of this study is the investigation of the most significant constructs that contribute to professional employees' (non-students) CMI in government agency environment.

This investigation also contributes to the IS and cybersecurity practice in that it provides valuable information that can be used in government agencies in an effort to significantly reduce computer user's misuse and, therefore, increase productivity and effectiveness. With computer abuse being reported in more than half of the business environments surveyed by the Computer Security Institute (CSI), computer user's misuse is problematic and continues to significantly increase. With this investigation and the existing body of knowledge, government agencies may be better positioned to understand and reduce computer users' misuse, starting with reducing their CMI.

Study Limitations

Like any other empirical research, this study also had several limitations. Three limitations were identified for this study. First, the study was comprised of working professionals at a single local government agency located in the northeastern U.S. Non-government organizations and government agencies of other states or countries were not covered in this study. Second, the survey for this study was completed within a four-week timeframe. Leonard and Cronan (2005) stated that a longitudinal study is needed as CSE, CCA, and CS influence may shift over time. Organizations must periodically reassess their employee's CSE, CCA, and CS and adjust the constructs that influence CMI (Leonard & Cronan, 2005). Third, self-reported CMI were measured instead of actual behaviors. Prior research indicates there is a reluctance of survey participants to report computer misuse (Foltz, 2004; Parker, 1998; Straub, 1990). While there is a significant body of research in IS (Ajzen, 1975; Davis, Bagozzi, & Warshaw, 1989) supporting intention as a predictor of actual behavior, actual behavior could be tracked by system monitoring tools instead of self- reported CMI. While actual misuse behaviors are difficult to measure, it is still measure that needs to be done by future work.

User awareness of computer sanctions (UAC-S) was initially included in this study, but it was removed due to some survey issues. The agency was concerned about the questions asked in UAC-S that might not comply with the agency's strict union rules. Another issue was that the expert panel reviewing the survey were concerned that the overall instrument was too long. The survey had 51 questions not including the UAC-S' six questions. Therefore, it was decided to rely on D'Arcy et al. (2009), Hovav and D'Arcy (2012), as well as Pahnila et al. (2007) research on the role of UAC-S in CMI. They found that perceived severity of sanctions was associated with reduced CMI, but perceived certainty of sanctions was not a significant predictor of CMI. In addition, they also stated that UAC-S may be significantly different across national cultures (e.g., U.S. vs. Korea). Additional work may investigate the role of UAC-S, if possible, in CMI.

The R-squared (R^2) of the latent variables on CMI was found to be 0.296 or nearly 30%. Wetzels et al., (2009) suggested a global fit measure (GoF) for PLS path modeling as a geometric mean of the average communality and average R^2. They indicated three cut-off points for GoF which are GoF(small) = 0.1, GoF(medium) = 0.25, and GoF(large) = 0.36. This study's R-squared (R^2) fits within the GoF(medium) = 0.25 and GoF(large) = 0.36, while a higher R^2 might have been able to demonstrate more significant results, thus, additional work is needed to re-validate the model proposed on another group of participants and in other more diverse organizations.

Recommendations for Future Research

Many areas of future research were identified as a result of this work. This study investigated working professionals at a single local government agency. This study could be replicated at another government agency in another part of the country or level (e.g., federal, state, or local government agency). In addition, this study can be also replicated in a private sector business environment as compared to a government agency. Future research could also be completed by incorporating and measuring user awareness of computer sanctions (UAC-S) and its role in reducing users' CMI in organizations. Research of system monitoring tools could also be completed to determine the percentage of computer use in government agencies that is non-work related (i.e. cyber-slacking) and test for various security countermeasures that could reduce the nonproductive work in the agency. Finally, as noted in the results section, future research is recommended to assess the potential hyperbolic relations between CSE and CMI constructs to better understand their non-linear relationship.

Summary

This dissertation investigation addressed the problem of computer misuse intention (CMI) by employees in a government agency, which contributes to cybersecurity vulnerabilities. While computer technology is generally intended to increase employee productivity and effectiveness, that same computer technology may be used in negative ways that reduce productivity and increase cybersecurity vulnerabilities. Computer users play a large role in information security (Veiga & Eloff, 2007). Users are one of the weakest links in the information systems security chain because many users appear to have limited or no cybersecurity awareness and skills (Albrechtsen, 2007;

Clifford, 2008). Many users are complacent with potential computer security risks when protective technologies (e.g., antivirus software) are not used or installed in their computer. They are willing to accept the security risks rather than addressing them due to the nuisances caused by security measures and cost (Dinev et al., 2008). Most users are not aware of the importance of protecting computer information systems, and this lack of awareness is reflected in their negligence in cybersecurity practices (Thomson & Solms, 2005). D'Arcy and Hovav (2009) as well as Straub (1986) have suggested that additional research investigating the factors that influence CMI is needed. After completing a comprehensive literature review, three constructs were identified as possible factors that may contribute to employee CMI.

The first construct identified in the literature as a possible contributor to CMI was computer self-efficacy (CSE). Bandura (1977), Compeau and Higgins (1995), Fischera (1980), Levy and Green (2009), Marakas et al. (1998), McCoy (2010), and Piccoli et al. (2001) suggested that CSE is a construct that contributes to CMI. Therefore, the contribution of CSE to employee CMI in government agency was investigated.

The second construct identified in the literature as a possible contributor to CMI was cybersecurity countermeasures awareness (CCA). Additional research was suggested by Boss et al. (2009), D'Arcy et al. (2009), Lee and Lee (2002), Straub (1990), Straub and Welke (1998), Torkzadeh and Lee (2003), Wybo and Straub (1989), as well as Urbaczewski and Jessup (2002) to the contribution of UAS-P in reducing employee CMI. Thus, the contribution of CCA to employee CMI in government agency was also investigated.

The third construct identified in the literature as a possible contributor to CMI was cybersecurity skills (CS). Albrechtsen (2007), Aytes and Connolly (2004), Cone et al. (2007), Cronan et al. (2006), Drevin et al. (2007), as well as Ramim and Levy (2006) suggested that CS is a factor that contributes to CMI. Hence, the contribution of CS to employee CMI in government agency was investigated.

A predictive model was designed to assess employees' CMI in government agencies based on the contribution of CSE, CCA, and CS, as measured by their contribution to CMI. The four specific hypotheses addressed were:

H1: Computer self-efficacy (CSE) of users will show significant positive influence on the cybersecurity countermeasures awareness dimensions (UAS-P, UAS-T, & UAC-M).

H2a: User awareness of security policy (UAS-P) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H2b: User awareness of security-training programs (UAS-T) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H2c: User awareness of computer monitoring (UAC-M) will show significant positive influence on the three cybersecurity skills (CCS, CIS, & CAS).

H3: The three cybersecurity skills (CCS, CIS, & CAS) of users will show significant negative influence on Computer Misuse Intention (CMI).

H4a: Users' *age* will show no significant influence on Computer Misuse Intention (CMI).

H4b: Users' *gender* will show no significant influence on Computer Misuse Intention (CMI).

H4c: Users’ *job function* will show no significant influence on Computer Misuse Intention (CMI).

H4d: Users’ *education level* will show no significant influence on Computer Misuse Intention (CMI).

H4e: Users’ *length of working in the organization* will show no significant influence on Computer Misuse Intention (CMI).

H4f: Users’ *military veteran status (i.e. ‘yes’ or ‘no’)* will show no significant influence on Computer Misuse Intention (CMI).

To address the specific hypotheses above, a survey instrument was developed by using previously validated survey items from the following research pool: D’Arcy et al. (2009), Levy and Green (2009), Levy, (2005), Hovav and D’Arcy (2012), as well as Torkzadeh and Lee (2003). CSE was measured using a validated three-item instrument developed by Levy and Green (2009). UAS-T and UAS-P were measured by utilizing the five validated survey items developed by D’Arcy et al. (2009). UAC-M was measured by using the six validated survey items developed by D’Arcy et al. (2009). CCS was measured by utilizing the six validated survey items developed by Torkzadeh and Lee (2003). CIS and CAS were measured by using the six validated survey items developed Levy (2005). CMI was measured using a validated eight-item instrument developed by Hovav and D’Arcy (2012). The demographics were measured by using validated survey items recommended by the expert panel.

A conceptual research model was proposed (see Figure 1). Partial Least Square (PLS) was utilized to test predictive power. It was predicted that CSE, CCA, and CS would have a significant ($p<.05$) impact on user’s CMI. The results demonstrated that

UAC-M and CIS were significant contributor ($p<.05$) to CMI. CSE demonstrated a significant contribution ($p < .001$) to CCS while it did not show significant contribution to CMI.

Following the analyses, the results and conclusions were discussed. This study's implication and limitations were identified and discussed. Recommendations for future research were outlined to build on this research and add to the existing body of knowledge.

APPENDIX A

Survey Instrument

Please respond to each of the following statements.

Computer Self-Efficacy

A1. I am comfortable working with computers. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

A2. If I am given some training, I can learn to use most computer programs. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

A3. I can learn to use most computer programs just by reading the manuals and help. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

End-User Awareness of Security Policies

B1. My organization has specific guidelines that describe acceptable use of email. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

B2. My organization has established rules of behavior for use of computer resources. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

B3. My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

B4.My organization has specific guidelines that describe acceptable use of computer passwords. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

B5. My organization has specific guidelines that govern what employees are allowed to do with their computers. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

End-User Awareness of Security-Training Programs

C1. My organization provides training to help employees improve their awareness of computer and information security issues. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

C2. My organization provides employees with education on computer software copyright laws. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

C3. In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

C4. My organization educates employees on their computer security responsibilities. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

C5. In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

End-User Awareness of Computer Monitoring

D1. I believe that my organization monitors any modification or altering of computerized data by employees. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

D2. I believe that employee computing activities are monitored by my organization. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

D3. I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

D4. I believe that my organization reviews logs of employees' computing activities on a regular basis. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

D5. I believe that my organization conducts periodic audits to detect the use of unauthorized software on its computers. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

D6. I believe that my organization actively monitors the content of employees' e-mail messages. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

E. Computer User Intentions

Scenario 1: Taylor is a manager in a company where he was recently hired. His department uses inventory application software to make inventory purchases. To ensure that only authorized individuals make inventory purchases, the company has a firm policy that employees must log out or lock their computer workstation when not in use. However, to make work more convenient, Taylor's boss directs him to leave his user account logged-in for other employees to freely use. Taylor expects that keeping his user account logged-in could save his company time.

INT1a. If you were Taylor, what is the likelihood that you would have kept your user account logged-in in order to save your company time? *

	1	2	3	4	5	6	7	
Very unlikely	○	○	○	○	○	○	○	Very likely

INT2a. I could see myself keeping my account logged-in to save my company time if I were in Taylor's situation. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

Scenario 2: Alexandra is a supervisor in a company where she was recently hired. Her company has a strong policy that each computer workstation must be password-protected and that passwords are not to be shared. However, Alexandra is working out in the field for the week and one of her co-workers needs a file on her computer. She expects that sharing her password could save her company a lot of time. Alexandra shares her password with her co-worker.

INT1b. If you were Alexandra, what is the likelihood that you would have shared your password with co-workers to save your company a lot of time? *

	1	2	3	4	5	6	7	
Very unlikely	○	○	○	○	○	○	○	Very likely

INT2b. I could see myself sharing my password with co-workers to save my company a lot of time if I were in Alexandra's situation. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

Scenario 3: Jordan is given a personal computer (PC) at work. The new PC came with a label containing her username and password. Jordan believes it would make her more effective on the job by leaving the username and password as it is since she has too many passwords, while it is difficult to remember them all. Jordan leaves her username and password visible.

INT1c. If you were Jordan, what is the likelihood that you would have left your username and password visible? *

	1	2	3	4	5	6	7	
Very unlikely	○	○	○	○	○	○	○	Very likely

INT2c. I could see myself leaving my username and password visible if I were in Jordan's situation. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

Scenario 4: Chris is a manager in a company where he has worked for several years. Chris is currently working on a report that requires the analysis of the company's employee database. This database contains employees home addresses, names, phone numbers, and social security numbers. Chris will travel for several days and would like to analyze the database on the road. Chris expects that copying the data to his personal USB drive and taking it on the road could save the company a lot of time and money. Chris copies the corporate database to his portable USB drive and takes it with him for the travel.

INT1d. If you were Chris, what is the likelihood that you would have copied the data to your personal USB drive? *

	1	2	3	4	5	6	7	
Very unlikely	○	○	○	○	○	○	○	Very likely

INT2d. I could see myself copying the data to my personal USB drive if I were in Chris's situation. *

	1	2	3	4	5	6	7	
Strongly disagree	○	○	○	○	○	○	○	Strongly agree

Cybersecurity Computing Skill

F1. Detecting and removing computer virus and worm. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

F2. Identifying and preventing computer phishing. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

F3. Installing and configuring a computer firewall. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

F4. Encrypting data. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

F5. Installing operating system's security patches. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

F6. Creating computer user account with different access level. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

Cybersecurity Initiative Skill

G1. Making decisions that involve computer security. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

G2. Being personally involved/taking responsibility in protecting the computer. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

G3. Taking initiative in developing computer security skill. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

G4. Starting new projects or activities to protect computer data. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

G5. Seeking and exploiting opportunities to increase computer security. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

G6. Finding ways to improve computer operating system security. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

Cybersecurity Action Skill

H1. Being persistent in following security policies and procedures. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

H2. Working to meet security policies and procedures. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

H3. Committing self to security goals and objectives. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

H4. Managing operating system security updates. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

H5. Organizing day-to-day computer security checking activities. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

H6. Making decisions in implementing new security tools. *

- No skill or ability.
- I am now learning this skill.
- I can do this skill with some help from a supervisor.
- I am a competent performer in this area.
- I am an outstanding performer in this area.
- I am an exceptional performer in this area.
- I am a leading performer in this area.

I. Demographics

I1. Age *

- Under 20
- 20-29
- 30-39
- 40-49
- 50-59
- 60 and over

I2. Gender *

- Female
- Male

I3. Job function *

- Administrative staff
- Managerial
- Officer
- Operations
- Security operator
- Technical
- Professional staff
- Other: ______

I4. How long have you been working in your current organization *

- Under 1 year
- 1-5 years
- 6-10 years
- 11-15 years
- 16-20 years
- 21-25 years
- 26-30 years
- over 30 years

I5. Education Level *

- High School Diploma
- 2-years college (AA degree)
- 4-years college/university (Bachelor's degree)
- Graduate (Masters degree)
- Doctorate degree
- Other: ______

I6. Veterans *

A veteran is a person who served in the active military, naval, or air service, and who was discharged or released therefrom under conditions other than dishonorable.

- Yes
- No

APPENDIX B

Approval Letter to Collect Data from the Agency

February 24, 2012

To Whom It May Concern:

Please be advised that Min Suk Choi has my permission to collect data from the computer end-users related to assessing the role of end-user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuse intention at government agencies in furtherance of his doctoral studies at Nova Southeastern University.

Please, let me know if you have any questions.

Sincerely,

Tariq Habib
Chief Technology Officer

APPENDIX C

IRB Approval Letter

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Min Suk Choi

From: Ling Wang, Ph.D.
Institutional Review Board

Date: April 24, 2012

Re: *Assessing the Role of End-User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills toward Computer Misuse Intention at Government Agencies*

IRB Approval Number: wang04151201

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *inga@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

References

2010/2011 Computer crime and security survey. (2011, June 6). *InformationWeek.* Retrieved September 13, 2011, from http://analytics.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html

Aakash, T. (2006). Determinants of adverse usage of information systems assets: A study of antecedents of IS exploit in organizations. *Dissertation Abstracts International, 67*(6). (UMI No. 3221195).

Ajzen, I. (1989). *Attitude, structure, and behavior*. Hillsdale, NJ: Lawrence Erlbaum Associates.

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

Alm, J., & McKee, M. (2006). Audit certainty, audit productivity, and taxpayer compliance. *National Tax Journal, 59*(4), 801–816.

Alvarez, R. (2002). Confessions of an information worker: A critical analysis of information requirements discourse. *Information and Organization, 12*(2), 85–107.

Axelrod, W. (2006). Cybersecurity and the critical infrastructure: Looking beyond the perimeter. *Information Systems Control Journal, 6*. Retrieved February 22, 2010, from http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Documents/jpdf0603-Cybersecurity-Critical.pdf

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing, 16*(3), 22-40.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215.

Bandura, A. (1984). Recycling misconceptions of perceived self-efficacy. *Cognitive Therapy and Research, 8*(3), 231-255.

Bandura, A. (1986). *Social foundations of thought and action*. Englewood Cliffs, NJ: Prentice Hall.

Baum, J., Frese, M., & Baron, R. (2007). *The psychology of entrepreneurship. The* *organizational frontiers*. Mahwah, NJ: Lawrence Erlbaum Associates.

Benitez-Amado, J., Perez-Arostegui, M., & Tamayo-Torres, J. (2010). Information technology-enabled innovativeness and green capabilities. *The Journal of Computer Information Systems, 51*(2), 87-96.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*(2004), 253-264.

Blanke, S. (2008). A study of the contributions of attitude, computer security policy awareness, and computer self-efficacy to the employees' computer abuse intention in business environments. *Dissertation Abstracts International*, *69*(11). (UMI No. 3336919).

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

Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology, 11*(3), 279-295.

Caputo, D. (2010). Gender differences in assessing essential business information systems technology skills. *International Journal of Management and Information Systems, 14*(2), 31-38.

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.

Chau, P.Y. (2001). Influence of computer attitude and self-efficacy on IT usage behavior. *Journal of End User Computing, 13*(1), 26-33.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), 7-16.

Chin, W.W., & Todd, P. (1995). One the use, usefulness, and ease of use of structural equation modeling in MIS research: A note of caution, *MIS Quarterly, 19* (2), 237–246.

Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* New York, NY: HarperCollins Publishers.

Clifford, M. (2008). Approaches to user education. *Network Security, 2008*(9), 15-17.

Compeau, D., & Higgins, C. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

Compeau, D., Higgins, C., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *Management Information System Quarterly, 23*(2), 145-158.

Cone, B., Irvine, C., Thompson, M., & Nguyen, T. (2007). A video game for cyber security training and awareness. *Computers & security, 26*(1), 63-72.

Creswell, J. (2005). *Educational research: planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson Education, Inc.

Cronan, T., Foltz, C., & Jones, T. (2006). Piracy, computer crime, and IS misuse at the university. *Communications of the ACM, 49*(6), 84-90.

Crossler, R., & Belanger, F. (2006, September). The effect of computer self-efficacy on security training effectiveness. *Proceedings of the InfoSecD Conference'06,* Kennesaw, GA.

D'Arcy, J. P. (2006). Security countermeasures and their impact on information systems misuse. A deterrence perspective. *Dissertation Abstracts International*. (UMI No. AAT 3203001).

D'Arcy, J., & Hovav, A. (2007). Towards a best fit between organization security countermeasures and information systems misuse behaviors. *Journal of Information System Security, 3*(2), 4-30.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59-71.

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.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

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

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2008). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

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.

Dreu, C., & Nauta, A. (2009). Self-interest and other-orientation in organizational behavior: Implications for job performance, prosocial behavior, and personal initiative. *Journal of Applied Psychology, 94*(4), 913-926.

Drevin, L., Kruger, H., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26*(1), 36-43.

Dworkin, J., Larson, R., & Hansen, D. (2003). Adolescents' accounts of growth experiences in youth activities. *Journal of Youth and Adolescence, 32*(1), 17-27.

Farrell, G., & Riley, M. (2011). *Hackers take $1 billion a year as banks blame clients for crime*. Retrieved August 09, 2011, from http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.htm

Fischera, K. (1980). A theory of cognitive development: The control and construction of hierarchies of skills. *Psychological Review, 87*(6), 477-531.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior*. Reading, MA: Addison-Wesley.

Fornell, C., & Larcker, D. (1981), Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18* (1), 39–50.

Foltz, B. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security, 12*(2), 154-166.

Fowler, F. J., Jr. (2009). *Survey research methods.* (4th ed.). Thousand Oaks, CA: Sage.

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

Gefen, D. & Straub, D. W. (2005). A practical guide to factorial validity using PLS-Graph:tutorial and annotated example. *Communications of the AIS, 16*(1), 91–109.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York, NY: Elsevier.

Gravetter, F., & Wallnau, L. (2009). *Essentials of statistics for the behavioral sciences.* Belmont, CA: Wadsworth Publisher.

Haenlein, M., & Kaplan, A. (2004). A beginner's guide to partial least squares analysis. *Understanding Statistics, 3*(4), 283–297.

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination.* London, UK: Sage.

Havelka, D., & Merhout, J. (2009). Toward a theory of information technology professional competence. *The Journal of Computer Information Systems, 50*(2), 106-117.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49* (2), 99-110.

Kerlinger, F. N., & Lee, H. B. (2000). *Foundations of behavioral research* (4th ed.). 46 Holt, NY: Harcourt College.

Korukonda, A. (1992). Managerial action skills in business education: Missing link or misplaced emphasis? *Advanced Management Journal, 57*(3), 27-35.

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

Lee, S., Yoon, S., & Kim, J. (2008). The role of pluralistic ignorance in internet abuse. *The Journal of Computer Information Systems, 48*(3), 38-43.

Leonard, L., & Cronan, T. (2005). Attitude toward ethical behavior in computer use: A shifting model. *Industrial Management and Data Systems, 105*(9), 1150-1171.

Lerouge, C., Newton, S., & Blanton, J. E. (2005). Exploring the systems analyst skill set: Perceptions, preferences, age, and gender. *Journal of Computer Information Systems, 45*(3), 12-22.

Levy, Y. (2005). A case study of management skills comparison in online and on-campus MBA programs. *International Journal of Information and Communication Technology Education, 1*(2), 1-20.

Levy, Y. (2006). *Accessing the value of e-learning systems.* Hershey, PA: Information Science Publishing.

Levy, Y., & Green, B. (2009). An empirical study of computer self-efficacy and the technology acceptance model in the military: A case of a U.S. navy combat information system. *Journal of Organizational and End User Computing, 21*(3), 1-2.

Mangione, T. (1995). *Mail surveys: Improving the quality.* Thousand Oaks, CA: Sage

Marakas, G., Yi, M., & Johnson, R. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research, 9*(2), 126-164.

McCoy, C. (2010). Perceived self-efficacy and technology proficiency in undergraduate college students. *Computers & Education, 55*(4), 1614-1617.

Mertler, C., & Vannatta, R. (2001). *Advanced and multivariate statistical methods*. Los Angeles, CA: Pyrczak.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Proceedings from HICSS '07: The 40th Hawaii International Conference on System Sciences*. Waikoloa, HI: IEEE.

Parker, D. (1998). *Fighting computer abuse – A new framework for protecting information*. New York, NY: John Wiley & Sons.

Phelps, D. (2005). *Information system security: Self-efficacy and security effectiveness in Florida libraries.* Retrieved from ProQuest Dissertations & Theses. (ATT 3183102).

Piccoli, G., Ahmad, R., & Ives, B. (2001). Web-based virtual learning environments: A research framework and a preliminary assessment of effectiveness in basic IT skills training. *MIS Quarterly, 25*(4), 401-427.

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: An assessment. *Journal of Management Information Systems, 10*(2), 75-105.

Pryor, C., Cormier, C., Bateman, B., Matzke, B., & Karen, B. (2010). Evaluation of a school-based train-the-trainer intervention program to teach first aid and risk reduction among high school students. *The Journal of School Health, 80*(9), 453-460.

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4) 24-34.

Rank, J., Pace, J., & Frese, M. (2004). Three avenues for future research on creativity, innovation, and initiative. *Applied Psychology, 55*(4), 518-528.

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

Rosenzweig, P. (2012, May 24). *The alarming trend of cybersecurity breaches and* *failures in the U.S. government*. Retrieved May 31, 2012, from http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government

Ross, C. (2006). Training nurses and technologists for trauma surgery. *Journal of Trauma Nursing, 13*(4), 193-196.

Ruighaver, A., Maynard, S., & Chang, S. (2007). Organizational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Sekaran, U. (2003). *Research methods for business: A skill-building approach* (4th ed.). New York, NY: John Wiley & Sons.

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

Stevens, J. (2007). *Intermediate statistics: A modern approach.* New York, NY: Lawrence Erlbaum Associates.

Straub, D. W. (1986). Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment. *Dissertation Abstracts International, 48*(4), 813. (UMI No. 8710538)

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information System Research, 1*(3), 255–276.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *Management Information System Quarterly, 14*(1), 45–60.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly*, *22*(4), 441-469.

Trochim, W.M.K. (2006). *Design research methods knowledge base*. Retrieved June 14, 2012, from http://www.socialresearchmethods.net/kb/design.htm

Swinarski, M., & Parente, K. (2010). A study of gender differences with respect to internet socialization of adolescents. *Journal of Business and Economics Research 8*(6), 23-30.

Thomas, M. A. (2003). *Web-based surveys*. Columbus, Ohio: Ohio State University, Program Development and Evaluation department.

Thomson, K., & Solms, R. (2005). Information security obedience: A definition. *Computers & Security*, *24*(1), 69-75.

Torkzadeh, G., & Lee, J. (2003). Measures of perceived end-user computing skills. *Information & Management, 40*, 607-615.

Torkzadeh, G., Chang, J., & Demirhan, D. (2006). A Contingency model of computer and internet self-efficacy. *Information and Management, 43*(2006), 541-550.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security, 14*(3), 198-217.

Udo, G., Bagchi, K., & Kirs, J. (2010). An assessment of customers' e-service quality perception, satisfaction and intention. *International Journal of Information Management, 30*(6), 481-492.

United States Census Bureau. (2012). *Federal employees summary characteristics* [Data file]. Retrieved from http://www.census.gov/compendia/statab/2012/tables/12s0500.pdf

Urbaczewski, A., & Jessup, L. M. (2002). Does electronic monitoring of employee Internet usage work? *Association for Computing Machinery, 45*(1), 80–83.

Vallacher, R., & Wegner, D. (1987). What do people think they're doing? Action identification and human behavior. *Psychological Review, 94*(1), 3-15.

Veiga, A., & Eloff, J. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-273.

Wetzels, M., Odekerken-Schröder, G., & Van-Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly, 33*(1), 177-195.

White House. (2009). *Assuring a trusted and resilient information and communications infrastructure*. Retrieved February 22, 2010, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Wyatt, G. (1990). Risk-taking and risk-avoiding behavior: The impact of some dispositional and situational variables. *The Journal of Psychology, 124*(4), 437–447.

Wybo, M. D., & Straub, D. W. (1989). Protecting organizational information resources. *Information Resources Management Journal, 2*(4), 1–15.