Winter 12-14-2013

The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse

MinSuk Choi
, Nova Southeastern University

Yair Levy Ph.D.
Nova Southeastern University, levyy@nova.edu

Hovav Anat
Korea University Business School, anatzh@koea.ac.kr

The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse

Min Suk Choi
International Information Systems Security Certification Consortium, Inc., (ISC)²®, New York, NY, USA

Yair Levy[1]
Graduate School of Computer and Information Sciences, Nova Southeastern University, Ft. Lauderdale, FL, USA

Anat Hovav[2]
Korea University Business School, Seoul, South Korea

ABSTRACT

Cybersecurity threats and vulnerabilities are causing substantial financial losses for governments and organizations all over the world. Intentional and unintentional users' misuse of information systems (IS) resources represents 50% to 75% of cybersecurity threats. Computer Crime and Security Survey revealed that nearly 60% of security breaches occurred from inside the organization by authorized users. Computer users are deemed as one of the weakest links in the IS security chain. In this study, we examined the effect of user computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) on users' computer misuse intention (CMI) at a government agency. Our results show that the factor of users' awareness of computer monitoring (UAC-M) and cybersecurity initiative skill (CIS) were significant contributors to CMI. UAC-M and CSE were significant contributors to cybersecurity computing skill (CCS). Users' awareness of security policy (UAS-P) was a significant

[1] Corresponding author: levyy@nova.edu

[2] Corresponding author: anat098@yahoo.com

contributor to cybersecurity action skill (CAS). However, CSE had no direct influence on misuse behavior. We conclude the paper with discussion about the results along with suggestions for future research.

Keywords: Computer self-efficacy, Computer misuse intention, Cybersecurity computing skills, Cyber security initiative skills, Cyber security action skills, Information Security.

INTRODUCTION

A number of research studies have investigated the reasons for internal misuse of computer resources (e.g., D'Arcy at al. 2009; Hovav and D'Arcy 2012; Veiga and Eloff 2007). Prior studies examined users' motivation to engage in misuse using a variety of theoretical foundations such as deterrence theory (DT), protection motivation theory (PMT), and theory of planned behavior (TPB). However, limited attention has been given in research for thorough examination of the effect of employees' security skills level on their misuse behavior. Thus, in this paper, we focused on assessing the role of such skills by looking at additional interactions between constructs that are known in the literature such as user computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS), along with their impact on computer misuse intention (CMI) in organizations.

THEORY AND RESEARCH MODEL

The Computer Security Institute (CSI) found that intentional and unintentional insider misuse of information systems (IS) resources (i.e., computer misuse) represents a significant threat to organizations (Blanke 2008). Intentional insider misuse includes actions such as data manipulation, destruction, and theft (Willison and Warkentin 2013). Examples of unintentional

insider misuse are: accidental entry of incorrect data values which can threaten data integrity or actions of users who are simply careless, unmotivated, or poorly trained (Willison et al. 2013). Users have a major role in organizational information security (Veiga and Eloff 2007). Users often accept security risks when the security measures interfere with their work or when the implementation costs are high (Dinev, Goo, Hu, and Nam 2008). Moreover, "A computer user that is aware of the security threats of spyware will be more motivated to use an anti-spyware" (Dinev et al. 2008 p. 8). Similarly users' awareness of procedural and technical countermeasures is likely to reduce misuse intentions (D'Arcy and Hovav 2009; Hovav and D'Arcy 2012).

D'Arcy et al. (2009) examined the role of user awareness of security countermeasures on IS misuse. Blanke (2008) investigated employee's intention to commit computer misuse in business environments. Aakash (2006) reported on the antecedents of IS exploitation in organizations. While all these studies uncover antecedents to IS misuse, none of these have investigated the role of the users' specific skills and how they might impact such critical behaviors. Moreover, while there has been some studies in leading IS literature on computing skills, such as Torkzadeh and Lee (2003), who developed the measures of user computing skills, they haven't looked into the role of such skills in the context of IS security mitigation or misuse. As such, in this study we will use the aforementioned literature as foundation of this paper to propose and empirically validate a model that incorporates both awareness constructs and users computing skills as predictors of misuse. In addition, the rigorous exploratory analysis of this new concept provides sufficient evidence that the constructs measures presented in this study are distinct.

Computer Misuse Intention (CMI)

Individuals are said to "obey least-effort rules because they are cognitive machines that attempt to cheaply reach flexible objectives rather than to act perfectly towards fixed targets" (Besnard and Arief 2004 p. 261). Users are often resistant to security policies and bypass them, thus, exposing their organizations to data loss and cybercrime (Boss et al. 2009). This is because users often perceive compliance with security policies as costly (Bulgurcu et al 2010). The incompetence of users who underestimate the dangers inherent in their actions represents one of the biggest computer security problems (Rezgui and Marks 2008).

Technology savvy users do not automatically become cybersecurity savvy. In other words, users' cybersecurity skills do not automatically increase with knowledge of the technology (Cronan, Foltz, and Jones 2006). According to Cronan et al. (2006), based on a 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 cybersecurity awareness on ethical conduct, trust, risk, and privacy may positively impact users' CMI (Rezgui and Marks 2008; Veiga and Eloff 2007).

Cybersecurity Computing Skill (CCS)

CCS has been defined as the knowledge, ability, and experience of an individual to use protective applications (e.g., antivirus software) to protect computers, computer networks, and IS (Levy 2005). Cybersecurity computing skills (CCS) include the technical knowledge, ability, and experience of an individual to use the hardware and software required to implement information security (Lerouge, Newton, and Blanton 2005). According to Lerouge et al. (2005), IS users need

appropriate CCS set to effectively utilize cybersecurity functions and innovations. Since one of the causes of IS security failure is attributed to users' limited CCS (Ramim and Levy 2006), increasing users' CCS can help reduce human error and misuse of computer assets (Drevin et al. 2007).

Cybersecurity Initiative Skill (CIS)

Initiative is a psychological transition that helps transform individual work roles and responsibilities into desired outcomes (Rank, Pace, and Frese 2004). Initiative skill is a capacity to direct attention and effort over time toward a challenging goal (Dworkin, Larson, and Hansen 2003). We define cybersecurity initiative skills (CIS) as the knowledge, ability, and experience needed to seek out as well as take advantage of security software (e.g., antivirus programs) and best security practices (Levy 2005). Personal initiative is the combination of proactive, self-starting, persisting behaviors that workers perform to achieve their desired goals (Dreu and Nauta 2009). Activities such as cybersecurity training are experiences in which users develop CIS by learning how to make plans, overcome obstacles, and achieve desired goals (Dworkin et al. 2003).

Albrechtsen (2007) stated that a "user-involving security awareness program approach is much more effective for influencing user awareness behavior than general security awareness campaigns" (p. 283). Thus, many organizations initiate a general security campaign with hopes to educate and train users in cybersecurity (Coneet et al. 2007). Such general security campaigns include sending emails or notes to the users, or publishing security policies on the organization's Intranet. Unfortunately, these general security campaigns are vastly ignored by most users (Coneet et al. 2007). Many forms of cybersecurity awareness initiatives fail because they are

simple routines that do not require users to take initiative and apply security concepts (Coneet et al. 2007). Therefore, a carefully designed CCA program appears to be vital in an attempt to increase users' CIS (Coneet et al. 2007).

Cybersecurity Action Skill (CAS)

Cybersecurity action skill (CAS) is defined as the knowledge, ability, and experience an individual has to commit to objectives in order to meet security compliance (Levy 2005). An action involves a collection of commitments that are applied to objectives (Fischera 1980; Levy 2005). Therefore, actions must always be adapted to specific commitments (Fischera 1980). For example, every time a user recognizes a familiar computer application, the action is adapted to that specific application (Fischera 1980). Every time an action is carried out, even to achieve the same objectives, it is often performed slightly differently (Fischera 1980). Thus, users can control the relevant action variations to achieve the same objective (Fischera 1980). Action produces results, makes applications work, and causes events to occur (Korukonda 1992). Examples of actions in the context of cybersecurity may be: managing antivirus software, security updates, or compliance with security policies and procedures. Thus, users' CAS is important for positive cybersecurity outcome.

Cybersecurity skills (CS) correspond to the technical knowledge, ability, and experience of an individual about the hardware and software required to implement information security (Lerouge et al. 2005). According to Lerouge et al. (2005), IS users need an appropriate skill-set to effectively utilize cybersecurity functions and innovations. Similarly, Ramim and Levy (2006) found that one of the main causes of system failure is attributed to users' limited technology knowledge and skill. Based on the above findings, we posit that the more skills users have, the

more likely they are to follow policies and procedures, especially ones that require technical knowledge. Hence, we hypothesize that:

H1a: *Users' perceived CCS will have a negative influence on Computer Misuse Intention (CMI).*

H1b: *Users' perceived CIS will have a negative influence on Computer Misuse Intention (CMI).*

H1c: *Users' perceived CAS will have a negative influence on Computer Misuse Intention (CMI).*

User Awareness of Security Policy (UAS-P)

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 (Lee and Lee 2002). Straub (1990), based on survey of 1,211 organizations, found that 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, security fails (Boss et al. 2009).

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). Hence, we hypothesize that:

H2a: *User awareness of security policy (UAS-P) will reduce CMI.*

In addition, policy awareness could help increase users' interest in cybersecurity skills (Blanke 2008). IS security policies are likely to educate and reinforce organizational best practices, process, and procedure. For example, IS security policy awareness on email could educate the user to identify and properly address inappropriate attachments, email phishing or social engineering attempts. Thus, we suggest that security policy awareness will increase cybersecurity skills. Hence, we hypothesize that:

H2b: *User awareness of security policy (UAS-P) will have a positive influence on CCS.*

H2c: *User awareness of security policy (UAS-P) will have a positive influence on CIS.*

H2d: *User awareness of security policy (UAS-P) will have a positive influence on CAS.*

User Awareness of Security-Training Programs (UAS-T)

UAS-T pertains to security training programs. Security training programs focus on providing users with knowledge of the information security policies needed to perform required cybersecurity activities (D'Arcy et al. 2009). A UAS-T program includes ongoing efforts to convey awareness to users about cybersecurity risks in the organization, 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 and 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).

One of the noted causes of IS 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 IS security training programs are essential in helping users understand the impact of computer misuse (Blanke 2008; 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). Hence, we hypothesize that:

H3: *User awareness of security training (UAS-T) will reduce CMI.*

User Awareness of Computer Monitoring (UAC-M)

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). Studies from criminology and sociology found that monitoring and surveillance help deter users' computer misuse (Alm and McKee 2006). Computer monitoring deters users' computer misuse because it increases the perceived chances of detection and punishment for such behavior (D'Arcy et al. 2009). Thus, we hypothesize that:

H4a: *User awareness of security monitoring (UAS-M) will reduce CMI.*

H4b: *User awareness of security monitoring (UAS-M) will have a positive influence on CCS.*

Computer Self-Efficacy (CSE)

The construct of CSE proposed by Compeau and Higgins (1995) was based on the general concept of self-efficacy developed by 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, Yi, and Johnson 1998). Compeau and Higgins (1995) defined computer self-efficacy "as beliefs about one's ability to perform a specific behavior" (p. 146) and as "an individual's perception of his or her ability to use a computer in the accomplishment of a job task" (p. 193). In addition "perceived self-efficacy plays a pivotal role in this process of self-management because it affects actions not only directly but also through its impact on cognitive, motivational, decisional, and affective determinants" (Bandura et al. 2003 p. 769).

Individuals who are more confident in their computer skills are more likely to expect positive results in their computer use (Compeau and Higgins 1995). Individuals' judgment of their ability to complete a task using computers influences their decision on how they will use computers (Piccoli, Ahmad, and Ives 2001). Research has shown that CSE significantly influences an individual's decision to use computers to achieve various tasks (Compeau and Higgins 1995; Marakas et al. 1998). According to Bandura (1977, 1984), self-efficacy beliefs determine the goals individuals set for themselves, how much effort they devote, how long they persevere, and their resilience in the face of setbacks and failures. Self-efficacy to regulate positive and negative affect is accompanied by high efficacy to manage one's educational development (e.g., cybersecurity skills), to resist temptations for antisocial activities such as computer misuse (Bandura et al. 2003). Therefore, we posit that the higher a users' CSE the more likely they are to develop cyber security skills. Thus, we hypothesize that:

H5a: *Computer self-efficacy (CSE) of users has a positive influence on CCS.*

H5b: *Computer self-efficacy (CSE) of users will reduce CMI.*

Control Variables

Prior research found age and gender to affect misuse intentions. Our goal is to understand the influence of cybersecurity skills and CSE on misuse intentions beyond personal characteristics. Thus, we include age and gender as control variables. Figure 1 depicts the proposed model resulting from the above set of hypotheses.

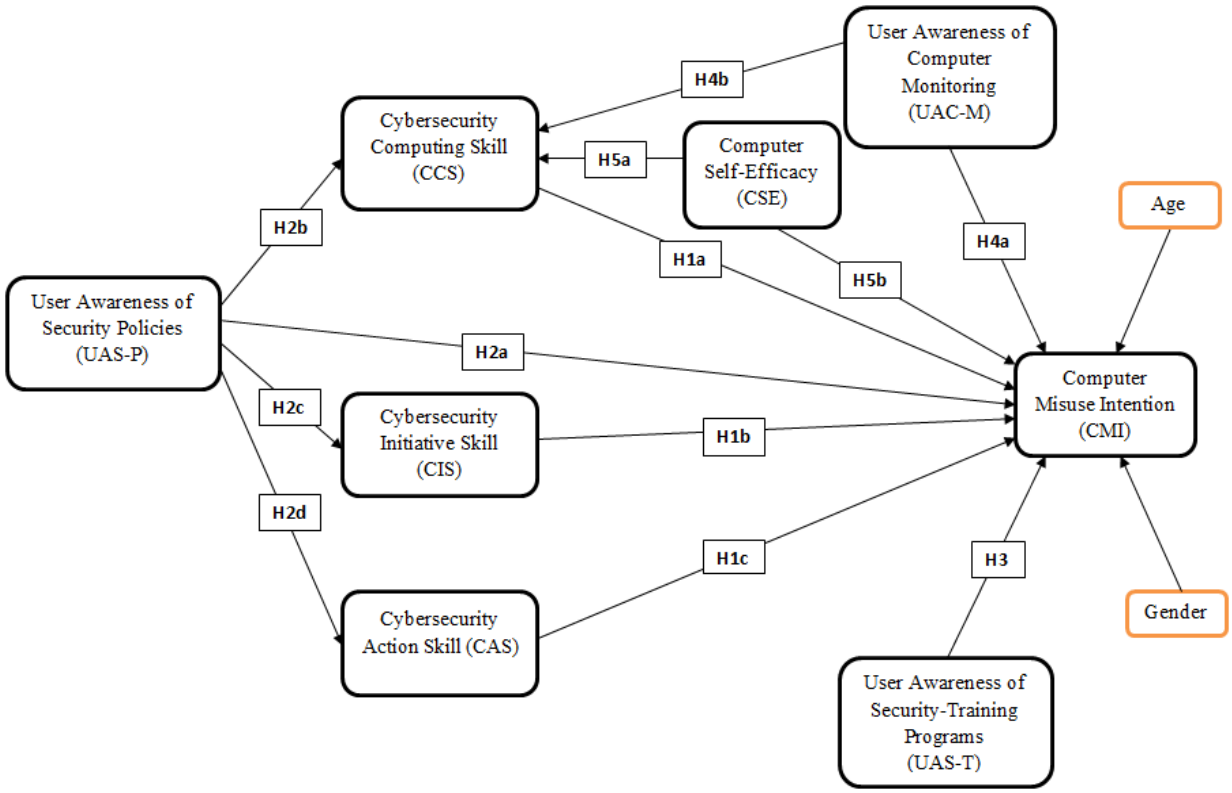

Figure 1. Research model for factors impacting CMI

DATA, ANALYSIS, AND RESULTS

An expert panel comprising of cybersecurity professionals reviewed the initial survey instrument. The expert panel evaluated the survey questions for relevancy, clarity of the questions, accuracy of the measurement instrument, and accuracy of the instructions. The expert panel consisted of three prominent cybersecurity professors and five practitioners that intensely

reviewed the survey instrument for validity. Additionally, the expert panel members were asked to provide recommendations for modifications and essentially performed a thorough examination of the instrument's validity. The feedback from the expert panel was used to adjust the instrument. In accordance with Straub (1989), adjustments included the removal of unnecessary, repetitive, or unclear items and/or the modification of questions, language, or layout of the instrument. The expert panel recommended only few minor wording adjustments, which were incorporated into the finalized survey instrument along with testing prior to data collection. The adjusted survey instrument was administered at a large government transportation agency in a Northeastern United States metropolitan (US). 185 responses were received.

Following data 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 along with the reliability of the constructs measured. The results demonstrated high reliability for all constructs measured (0.88 for CAS, 0.94 for CCS, 0.94 for CIS, 0.82 for CMI, 0.77 for CSE, UAC-M for 0.87 for UAS-P and 0.88 UAS-T). 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 a good representation of the population in the government agency we surveyed[3].

The data analysis was done using Partial Least Square (PLS) – Structural Equations Modeling (SEM) using SmartPLS. PLS was used to address the hypotheses and test the model fit. T-values have been obtained by running bootstrapping in SmartPLS. Based on our data with 184 degrees of freedom (df), T-values greater than 1.960 are significant at a p-value less than

[3] Additional information regarding the population analysis may be provided upon request

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 and Wallnau 2009). Table 1 shows the coefficient and T-value of each set of constructs path.

Table 1. Path coefficients significance (N=184)

Path	Hypotheses	Coefficients	T Statistics	Significant
CCS -> CMI	H1a	0.243329	1.952593	Supported (p<0.10)
CIS -> CMI	H1b	***-0.230363***	***1.973962****	Supported *(p< 0.05*)
CAS -> CMI	H1c	-0.152762	1.118844	Not supported
UAS-P -> CMI	H2a	-0.104848	0.808814	Not supported
UAS-P -> CCS	H2b	0.129809	1.625293	Not supported
UAS-P -> CIS	H2c	0.120009	1.663104	Supported (p<0.10)
UAS-P -> CAS	H2d	***0.219725***	***2.508762****	Supported (*p < 0.05*)
UAS-T -> CMI	H3	-0.166317	1.621924	Not supported
UAC-M -> CMI	H4a	***-0.190342***	***2.220108****	Supported (*p< 0.05*)
UAC-M -> CCS	H4b	***-0.178643***	***1.991473****	Supported[#] (*p< 0.05*)
CSE -> CCS	H5a	***0.391288***	***7.361295****	Supported (*p < 0.001*)
CSE -> CMI	H5b	-0.019187	0.212218	Not supported
Age -> CMI	N/A	-0.186975	1.719205	N/A
Gender -> CMI	N/A	-0.022814	0.262552	N/A

*p<0.05 (two-tailed tests)
**p<0.001 (two-tailed tests)
[#] - Reversed coefficient

Results of the standardized PLS path coefficients model for our study is presented in Figure 2.

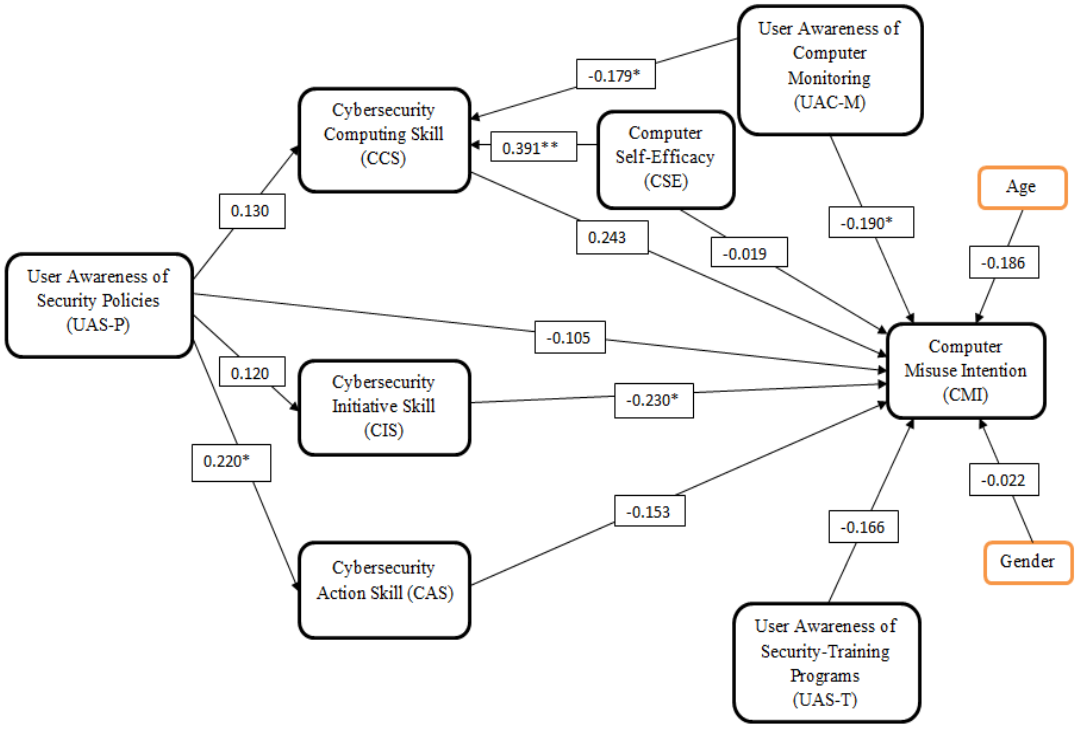

Figure 2. Results of the PLS-SEM analysis

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 control variables) (CIS → CMI, CSE → CSS, UAC-M→ CCS, UAC-M→ CMI, and UAS-P→ CAS) were significant at least at the p value of .05 level or greater ($p<0.001$). CCS → CMI and UAS-P → CIS were marginally supported at $p<0.10$. The rest of the model paths indicated path coefficients with non-significant p-values. The 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.

DISCUSSION

Our results show that UAS-P demonstrated a significant contribution to CAS. Our finding is consistent with the recommendations of IS security advocates who contend that security countermeasures awareness are important when it comes to cybersecurity skills. Interestingly, UAC-M demonstrated a significant negative contribution to CCS while our hypothesis suggested a positive relationship UAC-M → CCS, and may require further investigation. We suspect that such results are due to the fact that when individuals are being monitored, they're less likely to *explore* and *exploit* with the technology, which is less likely for them to cause any disruptive event in their organization, which ultimately they can't learn from their mistakes. Based on this finding, that UAC-M demonstrated a significant negative contribution to CCS, we speculate that while having no monitoring may not be the desired organizational solution at all, if monitoring can be done without the awareness of the employees, they may be able to learn from their mistakes when caught. Certainly, our interesting significant negative impact of UAC-M → CCS requires additional research and validation in the future.

One area that did not demonstrate significant contribution from CCA was CIS. This suggests that, in the context of the data collected in this paper, UAS-P increases users' CCS and CAS while it doesn't have a significant contribution to users' CIS. Interestingly, UAS-P showed strong contribution to CAS and marginal contribution to CIS. CIS showed significant contributions to CMI while CAS did not (See Figure 2). Also, CSE showed significant contribution to CCS while it did not show significant contribution to CMI. The non-significant results we found of CSE to CMI path align with prior research. Interestingly, CCS showed a positive relationship with CMI while our hypothesis suggested a negative relationship CCS→CMI. Prior studies (i.e., Hovav and D'Arcy 2009) speculated that computer savvy users

might feel that they can overcome organizational computer monitoring and other preventive measures, while 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. The path CSE→CCS→CMI sheds light on the relations between CSE and misuse intentions. The findings support the assertion that CSE influence on misuse intention is mediated by cybersecurity skills. Thus, computer savvy users are more likely to attempt misuse behavior when they have mastered relevant cybersecurity skills.

Monitoring was found to reduce misuse intentions. This is consistent with prior studies. CCS showed limited significant contribution 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 our study, 78.7% of the participants were 40 years old or more. Echt, Morrell, and Park (1998) study of two age groups found that age has an effect on training and computer skill acquisition. The younger group made fewer errors, required less help, and took less time to acquire the skills than the older group. Similarly, D'Arcy at al. (2009) found that age influences IS misuse intentions. Hovav and D'Arcy (2012) found that in the U.S. younger males were more likely to engage in CMI. Therefore, the impact of UAS-T on CS and CMI should be further investigated with a variety of professional computer users to investigate if the above results are age specific.

CONCLUSION

The purpose of this research was to assess the role of user computer self-efficacy (CSE), cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuse intention in organizations. This study addresses 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. Moreover, the results of our study indicate that user awareness of monitoring and cybersecurity initiative skill significantly reduces misuse intentions. Monitoring was found as a significant negative contributor to cybersecurity computing skill. User awareness of policies was found to significant increase cybersecurity action skills. Similarly, CSE demonstrated the most significant positive contribution to cybersecurity computing skills while it showed no significant contribution to misuse intentions.

REFERENCES

2010/2011 "Computer Crime and Security Survey." 2011. *Information Week.* Retrieved June 13, 2013, 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).

Albrechtsen, E. 2007. "A Qualitative Study of Users' View on Information Security," *Computers & Security* (26), pp. 276-289.

Alm, J., and McKee, M. 2006. "Audit Certainty, Audit Productivity, and Taxpayer Compliance," *National Tax Journal* (59:4), pp. 801–816.

Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices: A Rational Choice Perspective." *Journal of Organizational and End User Computing* (16:3), pp. 22-40.

Bandura, A. 1977. "Self-efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84:2), pp. 191-215.

Bandura, A. 1984. "Recycling Misconceptions of Perceived Self-efficacy," *Cognitive Therapy and Research* (8:3), pp. 231-255.

Bandura, A., Caprara, G., Barbaranelli, C., Gerbino, M., and Pastorelli, C. 2003. "Role of Affective Self-regulatory Efficacy in Diverse Spheres of Psychosocial Functioning," *Adolescent Psychology* (74:3), pp. 769-782.

Besnard, D., and Arief, B. 2004. "Computer Security Impaired by Legitimate Users," *Computers & Security* (23:2004), pp. 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., and 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), pp. 151-164.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Compeau, D., and Higgins, C. 1995. "Computer Self-efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.

Cone, B., Irvine, C., Thompson, M., and Nguyen, T. 2007. "A Video Game for Cyber Security Training and Awareness," *Computers & Security* (26:1), 63-72.

Cronan, T., Foltz, C., and Jones, T. 2006. "Piracy, Computer Crime, and IS Misuse at the University," *Communications of the ACM* (49:6), pp. 84-90.

D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89:1), pp. 59-71.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2008. User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences," *Information Systems Journal* (19:4), pp. 391-412.

Dreu, C., and 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), pp. 913-926.

Drevin, L., Kruger, H., and Steyn, T. 2007. "Value-focused Assessment of ICT Security Awareness in an Academic Environment," *Computers & Security* (26:1), pp. 36-43.

Dworkin, J., Larson, R., and Hansen, D. 2003. "Adolescents' Accounts of Growth Experiences in Youth Activities," *Journal of Youth and Adolescence* (32:1), pp. 17-27.

Echt, K., Morrell, R., Park, D. 1998. "Effects of Age and Training Formats on Basic Computer Skill Acquisition in Older Adults," *Educational Gerontology* (1:(24), pp. 3-25.

Fischera, K. 1980. "A Theory of Cognitive Development: The Control and Construction of Hierarchies of Skills," *Psychological Review* (87:6), pp. 477-531.

Gal-Or, E., and Ghose, A. 2005. "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16:2), pp. 186-208.

Gravetter, F., and Wallnau, L. 2009. *Essentials of Statistics for the Behavioral Sciences.* Belmont, CA: Wadsworth Publisher.

Kerlinger, F. N., and 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), pp. 27-35.

Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse within Organizations," *Information Management Computer Security* (10:2), pp. 57–63.

Lerouge, C., Newton, S., and Blanton, J. E. 2005. "Exploring the Systems Analyst Skill Set: Perceptions, Preferences, Age, and Gender," *Journal of Computer Information Systems* (45:3), pp. 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), pp. 1-20.

Levy, Y. 2006. *Accessing the Value of E-learning Systems.* Hershey, PA: Information Science Publishing.

Mangione, T. 1995. *Mail Surveys: Improving the Quality.* Thousand Oaks, CA: Sage.

Piccoli, G., Ahmad, R., and 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), pp. 401-427.

Ramim, M., and 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) pp. 24-34.

Rank, J., Pace, J., and Frese, M. 2004. "Three Avenues for Future Research on Creativity, Innovation, and Initiative," *Applied Psychology* (55:4), pp. 518-528.

Rezgui, Y., and Marks, A. 2008. "Information Security Awareness in Higher Education: An Exploratory Study," *Computers & Security* (27:7-8), pp. 241–253.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information System Research* (1:3), pp. 255–276.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Thomson, K., and Solms, R. 2005. "Information Security Obedience: A Definition," *Computers & Security* (24:1), pp. 69-75.

Torkzadeh, G., and Lee, J. 2003. "Measures of Perceived End-user Computing Skills," *Information & Management* (40:1), pp. 607-615.

Veiga, A., and Eloff, J. 2007. "An Information Security Governance Framework," *Information Systems Management* (24:4), pp. 361-273.

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

Willison, R., and Warkentin, M. 2013 "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.