2017

Gender Difference and Employees' Cybersecurity Behaviors

Mohd Anwar

Wu He
Old Dominion University, whe@odu.edu

Ivan Ash
Old Dominion University, iash@odu.edu

Xiaohong Yuan

Ling Li
Old Dominion University, lli@odu.edu

See next page for additional authors

Original Publication Citation

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. doi:10.1016/j.chb.2016.12.040

Gender difference and employees' cybersecurity behaviors

Article *in* Computers in Human Behavior · December 2016

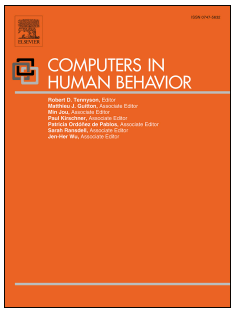
DOI: 10.1016/j.chb.2016.12.040

6 authors, including:

Mohd Anwar
North Carolina Agricultural and Technical State…
58 PUBLICATIONS **364** CITATIONS
SEE PROFILE

Wu He
Old Dominion University
111 PUBLICATIONS **1,642** CITATIONS
SEE PROFILE

Accepted Manuscript



Gender difference and employees' cybersecurity behaviors

Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, Li Xu

PII: S0747-5632(16)30868-8

DOI: 10.1016/j.chb.2016.12.040

Reference: CHB 4650

To appear in: *Computers in Human Behavior*

Received Date: 6 May 2016

Revised Date: 8 October 2016

Accepted Date: 18 December 2016

Please cite this article as: Anwar M., He W., Ash I., Yuan X., Li L. & Xu L., Gender difference and employees' cybersecurity behaviors, *Computers in Human Behavior* (2017), doi: 10.1016/j.chb.2016.12.040.

Gender Difference and Employees' Cybersecurity Behaviors

Mohd Anwar, Ph.D.
Assistant Professor of Computer Science
North Carolina A&T State University
Greensboro, NC 27411

Wu He, Ph.D.
Assistant Professor in the Department of Information Technology
Old Dominion University, Norfolk, VA

Ivan Ash, Ph.D.
Assistant Professor, Psychology Department
Old Dominion University, Norfolk, VA

Xiaohong Yuan, Ph.D.
Professor of Computer Science
North Carolina A&T State University
Greensboro, NC 27411

Ling Li
Professor, Information Technology & Decision Sciences
Old Dominion University, Norfolk, VA

Li Xu
Professor, Information Technology & Decision Sciences
Old Dominion University, Norfolk, VA

Gender Difference and Employees' Cybersecurity Behaviors

Abstract

Security breaches are prevalent in organizations and many of the breaches are attributed to human errors. As a result, the organizations need to increase their employees' security awareness and their capabilities to engage in safe cybersecurity behaviors. Many different psychological and social factors affect employees' cybersecurity behaviors. An important research question to explore is to what extent gender plays a role in mediating the factors that affect cybersecurity beliefs and behaviors of employees. In this vein, we conducted a cross-sectional survey study among employees of diverse organizations. We used structural equation modelling to assess the effect of gender as a moderator variable in the relations between psychosocial factors and self-reported cybersecurity behaviors. Our results show that gender has some effect in security self-efficacy ($r=-.435$, $p< .001$), prior experience ($r=-.235$, $p< .001$) and computer skills ($r=-.198$, $p< .001$) and little effect in cues-to-action ($r=-.152$, $p< .001$) and self-reported cybersecurity behaviors ($r=-.152$, $p< .001$).

Keywords: Gender differences, cybersecurity beliefs, cybersecurity behaviors, cybersecurity behavior model

1. Introduction

The information security community has come to realize that the weakest link in a cybersecurity chain is human (Sasse, 2005). To develop effective cybersecurity training programs for employees in the workplace, it is necessary to understand the security behavior of both men and women, and the similarities and differences of their security behaviors. According to U.S. Department of Labor's Bureau of Labor Statistics in 2010, women comprised 47 per cent of the total U.S. labor force and 66 million women were employed in the U.S. Gender is one of the most fundamental groups and membership in such a group is likely to have a profound influence on an individual's perceptions, attitudes, and performance (Nosek, Banaji, & Greenwald, 2002). As a result, studying the role that gender plays with respect to cybersecurity beliefs and behaviors is very important.

Morris, Venkatesh, & Ackerman (2005) studied gender differences in technology adoption and use in workplace and found that gender differences were more pronounced with increasing age. Specifically, gender differences in technology perceptions became more pronounced among older workers and less pronounced among younger workers. Several studies show that gender is related to the degree of online privacy concerns and females show greater privacy concerns than males (Hoy & Milne, 2010; Laric, Pitta, & Katsanis, 2009). Herath & Rao (2009) found that gender has a significant correlation on employees' policy compliance intentions and females have higher policy compliance intentions than males. Ifinedo (2014) found that males appeared to have lower security policy compliance intentions compared to females and suggest that practitioners pay attention to gender differences in relation to security policy compliance in organizations. Targeted security awareness program and monitoring are also suggested to bridge gaps in security behavior between male and female (Ifinedo, 2014). However, a recent study by Vance, Siponen, & Pahnila (2012) surveyed a Finnish municipal organization and received 210 survey responses from 22% male and 78% female employees. The survey results did not reveal any gender difference in employees' intention to comply with information system's security policies.

Theories such as the Health Belief Model (Rosenstock, 1974) and Protection Motivation Theory (Rogers, 1983) have been used primarily to explain users' intention to employ security technologies, and how and when a user adopts adaptive or maladaptive behaviors when he/she is informed of a threatening security incident. Health belief model (HBM) is a conceptual model developed to explain why people do not participate in health behaviors. The components of HBM include perceived susceptibility, perceived severity, perceived benefits, perceived barriers, and cues to action. Protection motivation theory (PMT) is an extension and reworking of HBM. PMT considers intention to protect oneself as the determinant of health behavior, and intention is dependent on perceived susceptibility, perceived severity, self-efficacy, and response-efficacy.

Guided by these theories, recent empirical studies (Mohamed & Ahmad, 2012; Ng, Kankanhalli & Xu, 2009; Pahnila, Siponen, & Mahmood, 2007) in information security also found that perceived susceptibility, perceived severity, perceived benefits, and self-efficacy are correlated with security behaviors. In addition, other studies (Vance, Siponen, & Pahnila, 2012; Son, 2011; Herath & Rao, 2009) show that perceived barriers, peer behavior, cues to action (i.e., experiences or triggers that would motivate and activate a user to practice computer security), past security compliance habits and personal factors (e.g., gender, education level) also have some effects on users' security behavior. Other studies also found that computer skills, information seeking skills, and prior experience with computer security practices (Ng, Kankanhalli & Xu, 2009) can predict a person's security behavior (Wan, Wang & Haggerty, 2008).

The prior research has revealed evidence of gender differences surrounding beliefs and behavioral intentions regarding cybersecurity. Following the prior research studies, there is a need for more research investigating the similarities and differences of the cybersecurity beliefs and behavior among men and women. Furthermore, research has applied psychological factors

that have been developed to explain health related behaviors to the domain of cybersecurity. Therefore, this research investigated the relations between gender and the components of the proposed cybersecurity behavior model (Figure 1), which is based on Protection Motivation Theory and Health Belief Model. Thus, we conducted a survey study to investigate the relations between gender and these factors of the model. Five-hundred-seventy-nine (579) employees from various U.S. organizations and companies completed an online survey with 87 Likert scale survey items. The survey items are drawn from the perspectives of cybersecurity, information technology, and psychology and decision science. Many of these survey items are designed anew while the rest are adapted from the literature. The results from data analysis of the survey data are presented in this paper.

2. Theory and Research Question

Adapting from the Health Belief Model (Rosenstock, 1974) and Protection Motivation Theory (Rogers, 1983), we studied following constructs: security self-efficacy (SSE), perceived severity (PS), perceived vulnerability (PV), perceived benefits (PB), computer skills (CS), Internet skills (IS), prior experience with computer security (PE), perceived barriers (PBR), response efficacy (RE), cues to action (CA), peer behavior (PBEH), and self-reported cybersecurity behavior (SRCB). Higher mean values for perception constructs represent higher perception levels. The goal of this study is to investigate into the differences between male and female (gender as a moderating variable) in terms of the above-stated constructs affecting cybersecurity beliefs and behaviors.

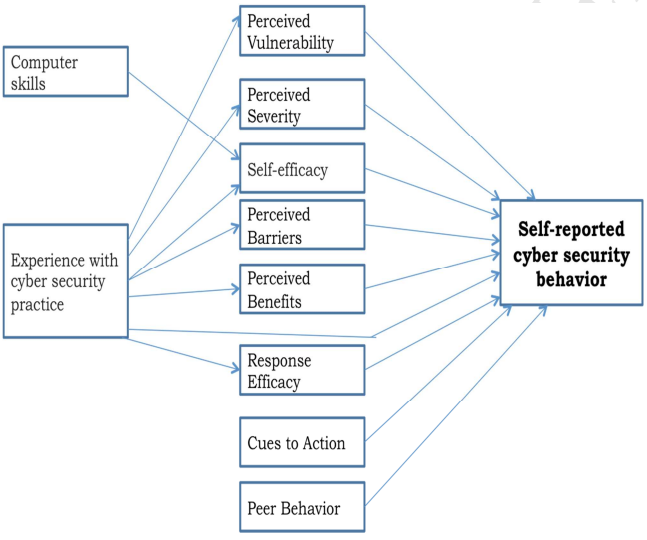


Fig. 1. Cybersecurity behavior model

The research question that we sought to explore is whether differences in cybersecurity beliefs and behaviors exist based on gender. We test the hypothesis that there is a difference in cyber-security beliefs and behaviors between male and female employees. To test this hypothesis, we conducted survey-based experiments among employees of different organizations (IT companies, academia, government institutions, etc.). These employees were asked various questions related to the perceptions of various key constructs of our cybersecurity behavior model. Likert items are used to measure the survey participants' perceptions/attitudes to a particular question. The responses are coded on a continuum from 1 (strongly disagree) to 7 (strongly agree). The constructs are quantified by calculating the means of the numerical codes from the responses. Our findings offered more fine-grained understanding of user and their motivation as well as would help design appropriate interventions.

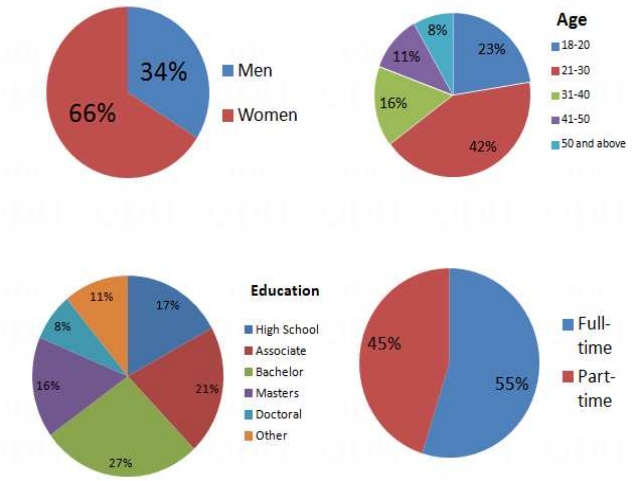


Fig. 2. Demographic statistic

Table 1. Result of experiments Means, standard deviations, and point-biserial correlation with self-report genders for the different self-report cyber security scales (i.e., Computer Skills (CS), Internet Skills (IS), Prior Experience (PE), Perceived Vulnerabilities (PV), Perceived Severity (PS), Perceived Benefits (PB), Perceived Barriers (PBR), Response Efficacy (RE), Cued to Action (CA), Security Self-efficacy (SSE), Peer Behavior (PBEH), Self-reported Cybersecurity Behavior (SRCB))

	Men (N =163)		Women (N = 318)			
	M	SD	M	SD	r	P
CS	5.23	0.79	4.90	0.78	-.198	< .001
IS	4.95	0.66	4.82	0.63	-.101	.026
PE	5.10	1.17	4.44	1.33	-.235	< .001
PV	4.56	1.08	4.32	1.04	-.111	.015
PS	4.44	1.62	4.84	1.61	.116	.011
PB	5.59	1.02	5.74	0.92	.076	.096

PBR	3.43	1.39	3.45	1.32	.006	.898
RE	5.47	0.95	5.56	0.89	.047	.047
CA	4.29	1.56	3.78	1.57	-.152	< .001
SSE	5.07	1.32	3.73	1.46	-.435	< .001
PBEH	4.30	1.30	4.09	1.25	-.081	.076
SRCB	5.61	0.86	5.31	0.93	-.152	< .001

3. Methodology

2.1 Participants and Setting

In June 2014, we sent out this online survey to employees in various organizations and invited employees to participate in the online survey about their experiences and beliefs with computer and Internet security. As a result, 579 subjects from businesses and university subject pools completed the survey. However, we removed the data points corresponding to university students without outside employments. Four-hundred-eighty-one (481) participants from this sample were employed full or part time. In order to increase the validity of the study, only the sample of full and part time employees were used in all analyses. As table 2 shows, a chi-square test revealed no significant difference in the proportion of men and women at each age category, X^2 (4, N = 481) = 5.41, p = .248.

All volunteers received information about the purpose and procedure to participate in this study. The consent form included the following sentences about the role of usage and anonymity of responses: Identifying information is collected for data validity and management purposes, and will be removed after the data is collected. No names will be attached to the questionnaire and the interview. The participants gave their consents before participating in the survey. The Internal Review Board (IRB) of the investigators' institutions approved the study.

The key criterion for inclusion was that the participants work full-time or part-time and their job requires the use of technology.

2.2 Measurement

Based on a thorough literature review on articles related to behavioral information security and the proposed model, we designed a survey as the instrument for data collection about employees' security behavior. This survey instrument was tested through a pilot survey study with 197 students from late 2013 to early 2014 at a state university in Virginia, USA. The pilot study results were used to check the wordings and relevance of each item and help us refine the items as needed. The behavior and belief variables in the final version of the survey are assessed on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7). The final survey includes 87 Likert items collecting data to measure an individual's computer skills, self-efficacy, prior experience with computer security practice, and other elements depicted in the proposed model. The actual survey questionnaires are presented in appendix A. Items to measure each latent variable in the research model were developed by either adopting or modifying questionnaires from existing literature. For example, measures to test security self-efficacy were adapted from Rhee, Kim & Ryu (2009), Ifinedo (2014) and Ng,Kankanhalli, & Xu (2009). Items to assess self-reported cyber security behaviour were adapted from Vance, Siponen, & Pahnila (2012), Shih, Lin,Chiang, & Shih (2008), Davinson & Sillence (2010), and Ng, Kankanhalli, & Xu (2009).

Data were analyzed using IBM'S statistical analysis software package, SPSS (version 2015).

3. Results

Demographic Statistic. Sixty-six percent of the respondents were women and thirty-four percent are men. Figure 2 summarizes demographic statistics of the employee sample. Across genders, 21% of the participants had an associate degree and 27% of the respondents had a bachelor's degree. Besides 8% of participants had a PhD degree and 16% of the participants have a master's degree. Forty-five per cent (45%) of the sample reported having a part-time position and 55% reported having a full time job. The majority of the participants (Forty-two per cent) are between the ages of 21-30. There are 8% participants between ages 50 and above. Job responsibility ranges from senior manager, middle manager to administrative support. The participants come from different types of organizations including government, education, finance, information technology, retail, real estate, telecommunication, healthcare and military.

When the respondents were asked if his/her company had an explicit cybersecurity policy in place, about 49% of the participants answered "yes," 15% answered "no," and about 36% had no knowledge about their company's information security policy. Respondents' industry includes retail and wholesale, healthcare and medicine, finance, information technology, education, real estate, telecommunication, military and others. The company size can ranges from more than 1,000 people to as small as 20 or fewer.

Table 2. Age-wise gender distribution of participants

			Gender		
			Men	Women	Total
Age	18-20	F	27	81	108
		%	16.6%	25.5%	22.5%

21-30	f	74	130	204
	%	45.4%	40.9%	42.4%
31-40	f	30	46	76
	%	18.4%	14.5%	15.8%
41-50	f	18	35	53
	%	11.0%	11.0%	11.0%
51 +	f	14	26	40
	%	8.6%	8.2%	8.3%

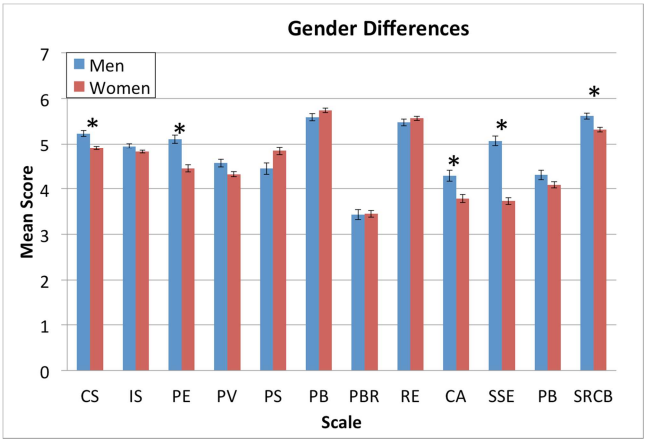


Fig. 3. Gender differences for the different self-report cybersecurity scales.

3.2 *Gender Differences.*

The relationship of gender with the Cyber-security scales was accessed with a series of biserial point correlations with gender coded as 1 for women and 0 for men (see Table 1). Due to the large sample size (n=481) and exploratory nature of this study we only discuss results that were significant at an alpha level of < 0.01, in order to avoid over interpreting relationships with effect sizes. Women self-reported slightly lower levels of computer skills, lower prior experience with computer security, and lower cues to action scores. The largest difference between men and women was observed on security self-efficacy, where women's mean self-efficacy score was .95 standard deviations lower than men's mean ratings. Women also self-reported lower cyber security behaviors scores. However, this effect was not nearly as large as the difference between genders on self-efficacy. These results suggest that men and women have differences in their perceived computer abilities. However, it is unclear whether their actual cyber security behavior differs from men or whether it is just a function of overconfidence in the men in the sample or under confidence in the women in the sample.

In summary, there are five gender effects: Computer Skill, Prior Experience, Cues to Action, Security Self Efficacy, and Self Report Cyber-security behavior. The biggest effect is Security Self Efficacy (r=-.435, p< .001) and the smallest effect is cues-to-action (r=-.152, p< .001).

3.3 *Gender Interactions:*

The observation that there are significant differences between men and women on a number of the Health Belief Model (Rosenstock, 1974) and Protection Motivation Theory (Rogers, 1983) inspired cybersecurity belief measures raises the question whether men's and women's responses on this scale have different relationships with self-reported cybersecurity behavior. In order to investigate this question a series of regression analyses testing the interaction between each predictor variable and gender on the relationship with self-reported cybersecurity behavior were conducted. For all analyses, interaction terms were constructed by centering each predictor variable on its' mean and calculating the centered score's product with the binary gender variable. Table 1 reports the correlations between each of the predictor variables and self-report cyber security behaviors as a function of gender, and reports the significance test for the interaction term in each regression model. Again, we adopted an alpha level of less than 0.01 for all analyses. Although the correlations showed some variability across men and women, none of these differences approach statistical significance. This suggests that while men's and women's scores on many of these variables differ, the overall relationships among the variables do not differ. This suggests that the same theoretical or predictive models of self-report cyber-security behaviors may be able to be applied to both men and women employees.

Discussion.

Most of the prior studies (e.g., Sheehan, 1999; Hoy & Milne, 2010; Laric, Pitta, & Katsanis, 2009; Herath & Rao, 2009; Ifinedo, 2014) have shown that women are generally more concerned about privacy (perceived vulnerability) than men and are more likely to comply with security policy than men. However, this research study reveals that men have slightly higher self-reported cybersecurity behavior (mean = 5.61, SD = .86) than women (mean = 5.31, SD = .93).

Morris et al. (2005) studied adaption and sustained use of technology in the workplace. Their study found that men place greater influence on attitude toward using technology than women while women were more driven by subjective norms, social roles, and behavioral control. However, it is not clear how these factors of technology use moderate self-reported cybersecurity behaviors of men vs. women.

Additionally, Gustafsod (1998) found that women and men differ in their perceptions of risk. Dwyer et al. (2002) found that women have higher levels of concern about risks while men are more willing to take risks. Hajli and Lin (2016) found that women place significantly greater importance on perceived control and privacy risk when sharing information on social networking sites. However, our study found insignificant difference in perceived vulnerability (PV) (r=-.111, p= .015) between men (mean=4.56, SD=1.08) and women (mean=4.32, SD=1.04). Our study also contributes to the existing literature by discovering and explaining gender differences in the context of cybersecurity in organization environments.

Our study found that men and women self-reportedly behave differently, however we have not taken any actual objective measure of the participants' behaviors. Men self-reported better cybersecurity behavior than that of women, however if it is men's overconfidence then women are not more vulnerable to cybersecurity risks. The data from 481 employees are used in this point biserial correlation experiment, however for generalizability of the findings, we plan to run this experiment with a larger dataset in the future.

Conclusion. Gender is an important factor mediating human behaviors in general. Our research explores the role of gender in cybersecurity behaviors and beliefs. We compare the constructs of our cybersecurity behavior model between male and female employees in a cross-sectional survey study. The results show that there are statistically significant gender-wise differences in terms of computer skills, prior experience, cues-to-action, security self-efficacy and self-reported cybersecurity behavior. Since women's self-efficacy is significantly lower than men, women's self-efficacy may be a target for intervention. The practical application of our findings is to develop gender-specific cybersecurity training and interventions, targeting on the relevant constructs of the cybersecurity behaviour model to improve the attitudes and behaviours of employees.

References

Albion, P. (2007). Student teachers' confidence and competence for finding information on the Internet. In *Society for Information Technology & Teacher Education International Conference* (Vol. 2007, No. 1, pp. 1244-1249).

Anderson, C. L., & Agarwal, R. (2006). Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. In *International Conference on Information Systems* (pp. 1543-1561).

Aytes, K., & Connolly, T. (2005). Computer security and risky computing practices: A rational choice perspective. Advanced topics in end user computing, 4, 257-279.

Chan, M., I.M.Y. Woon, A. Kankanhalli (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior, Journal of Information Privacy and Security, 1(3), 18-41.

Davinson, N., and Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among Internet users. *Computers in Human Behavior*, 26(6), 1739-1747.

Dwyer, P. D., Gilkeson, J. H., & List, J. A. (2002). Gender differences in revealed risk taking: evidence from mutual fund investors. *Economics Letters*, 76, 151–158.

Erdelez, J. L. M., & He, W. (2007). The search experience variable in information behavior research. *Journal of the American Society for Information Science and Technology*, *58*(10), 1529-1546.

Gustafsod, P. E. (1998). Gender differences in risk perception: Theoretical and methodological erspectives. *Risk Analysis*, 18, 805–811.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, 133(1), 111-123.

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

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Mohamed, N., & Ahmad, I. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366–2375.

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005). Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior. *IEEE Transactions on Engineering Management*, 52(1), 69-84.

Nosek, B. A., Banaji, M., & Greenwald, A. G. (2002). Harvesting implicit group attitudes and beliefs from a demonstration web site. Group Dynamics: *Theory, Research, and Practice*, 6(1), 101.

Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. PACIS 2007 Proceedings, 45.

Ng, B.Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior using the health belief model. *Decision Support Systems*, 46(4), 815-825.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In Proceedings of 40th Annual Hawaii International Conference on System Sciences, pp. 156b-156b. IEEE.

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

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

Rosenstock, I. M. (1974). The health belief model and preventive health behavior. *Health Education Monographs* 2.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In: Cranor, LF and Garfinkel, S, (eds.) Security and Usability: Designing secure systems that people can use. (pp. 13 - 30). O'Reilly: Sebastopol.

Sheehan, K. B. (1999). Toward a Typology of Internet Users and Online Privacy Concerns. *Information Society*, 18(1), pp. 21-32.

Schulenberg, S. E., Yutrzenka, B. A., & Gohm, C. L. (2006). The computer aversion, attitudes, and familiarity index (CAAFI): A measure for the study of computer-related constructs. *Journal of Educational Computing Research*, *34*(2), 129-146.

Shih, D. H., Lin, B., Chiang, H. S., & Shih, M. H. (2008). Security aspects of mobile phone virus: a critical survey. *Industrial Management & Data Systems*, *108*(4), 478-494.

Smith, A. D. (2006). Exploring security and comfort issues associated with online banking. *International Journal of Electronic Finance*, *1*(1), 18-48.

Son, J.Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296-302.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49(3), 190-198.

Wan, Z., Wang, Y., & Haggerty, N. (2008). Why people benefit from e-learning differently: The effects of psychological processes on e-learning outcomes. *Information & Management*, 45 (8), 513-521.

Appendix A. Questionnaire Items

Constructs	Sample Items	References (Adapted from)
Computer Skills	What is your comfort level, when using computers? How would you evaluate your computer knowledge in general? How would you evaluate your computer skills in general? I am comfortable installing or upgrading computer software on my computer. I avoid using computers whenever possible. I know how to use computer files and folders.	Schulenberg, Yutrzenka, & Gohm (2006)
Internet Skills	What is your comfort level with the Internet? How would you evaluate your Internet skills in general? How comfortable are you with using your browser's bookmarks? How comfortable are you with using internet calling software (e.g., Skype)? How comfortable are you with social media (e.g., Facebook, Twitter, Google+, Blogs, LinkedIn)? How comfortable are you with using online systems for banking? How comfortable are you with using online systems for financial transactions (e.g., credit card transactions)?	Schulenberg, Yutrzenka, & Gohm (2006); Smith (2006)

	How comfortable are you with online shopping?	
Information-seeking skills using the Internet	I am confident in using the Internet to find information I need. I am confident in using online library databases to find information. I am confident in my skills of using multiple search engines (e.g., Google, Yahoo, Microsoft's Bing) to find information. I am confident in my skills of using Google's Advanced Search feature. When using the library catalog, I often combine keywords using AND, OR, or NOT.	Albion (2007); Erdelez, Moore, & He(2007)
Prior experience with computer security practices	I had formal training on common computer security practices. I read computer security-related newsletters or articles before. I used different passwords for different accounts. The organization I worked for had an established information security policy. The organization I worked for has provided employees with information security training. The organization I worked for has provided employees with security-related newsletters or articles.	Aytes & Connolly (2005); Ng,Kankanhalli, & Xu (2009)
Perceived vulnerability	I feel that my chance of receiving an email attachment with a virus is high. I feel that my chance of receiving malware on social media sites is high. I feel that my organization could become vulnerable to security breaches if I don't adhere to its information security policy. I feel that I could fall victim to a malicious attack if I fail to comply with my organization's information security policy. I believe that my effort to protect my organization's information will reduce illegal access to it. My organization's data and resources may be compromised if I don't pay adequate attention to information security policies and guidelines. It is likely that an information security breach is occurring at my workplace. It is likely that my organization's information and data is vulnerable to security breaches.	Ng,Kankanhalli, & Xu (2009); Mohamed & Ahmad (2012); Ifinedo (2012)
Perceived severity	Having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me. If I violate my organization's security policy, the sanctions would put me in serious trouble. At work, having my confidential information accessed by someone without my consent or knowledge is a serious problem for me. Loss of data resulting from hacking is a serious problem for me.	Ng,Kankanhalli, & Xu (2009); Ng & Xu (2007); Mohamed & Ahmad (2012); Ifinedo (2012)
Perceived benefits	I believe that checking the filename of the email attachment can help me avoid viruses that may infect my computer. I believe that compliance with my organization's information security policy will reduce the risk of losing valuable work.	Ng,Kankanhalli, & Xu (2009)

	Cyber security training makes me feel more equipped to deal with security problems on the computer. I believe that using strong passwords that are at least eight characters long and consist of some combination of letters, numbers, and special characters will make my online accounts (e.g., my online bank, Facebook or Twitter accounts) more secure. I believe that changing the default privacy and security settings on my social media sites (e.g., Facebook and Twitter) will make my personal information more secure. I believe that backing up important files on my computer will reduce my concern for security.	
Perceived barriers	It is inconvenient to check the security of an email with attachments. Changing the privacy setting on social media sites is inconvenient. Backing up a computer regularly is inconvenient. Cyber security training takes too much time from work.	Ng,Kankanhalli, & Xu (2009)
Response Efficacy	Complying with the information security policies in my organization will keep security breaches down. If I comply with information security policies, the chance of information security breaches occurring will be reduced. Careful compliance with information security policies helps to avoid security problems. Using information security technologies is an effective way to protect confidential information.	Vance, Siponen， & Pahnila (2012)
Cues to Action	My organization distributes security newsletters or articles. My organization organizes security talks and training. My organization's Information Technology helpdesk sends out alert messages/emails concerning security. My organization constantly reminds me to practice its computer and Internet security policies.	Ng,Kankanhalli, & Xu (2009)
Security Self-efficacy	My organization constantly reminds me to practice its computer and Internet security policies. I know how to apply security patches to operating systems. I feel confident in setting the Web browser to different security levels. I feel confident in handling virus-infected files. I feel confident in getting rid of spyware and malware from my computer. I have the skills to implement security measures to stop people from getting my confidential information. I have the skills to implement security measures to stop people from damaging my computer.	Rhee, Kim & Ryu (2009), Ifinedo (2014) and Ng,Kankanhalli, & Xu (2009).
Peer behaviour	My colleagues at work update their computers regularly. I believe other employees in my organization back up their computers regularly. I am convinced that other employees comply with the organization’s information security policy (if the organization has one). The majority of employees in my organization attend cyber security training.	Herath & Rao (2009); Anderson & Agarwal (2006); Chan, Woon, Kankanhalli(2005)
Self-reported	I use different passwords for my different social	Vance, Siponen， & Pahnila

cyber security behaviour	media accounts (e.g., Facebook, Twitter, LinkedIn). I usually review privacy/security settings on my social media sites (e.g., Facebook, Twitter, LinkedIn). I keep the anti-virus software on my computer up-to-date. I watch for unusual computer behaviors/responses (e.g., computer slowing down or freezing up, pop-up windows, etc). I do not open email attachments from people whom I do not know. I have never sent sensitive information (such as account numbers, passwords, and social security number) via email or using social media. I back up important files on my computer. I always act on any malware alerts that I receive. I don't click on short URLs posted on social media sites unless I know where the links will really take me.	(2012), Shih, Lin,Chiang, & Shih (2008), Davinson & Sillence (2010), and Ng,Kankanhalli, & Xu (2009).

Acknowledgments

This work was supported in part by the U.S. National Science Foundation under Grant SES-1318470 and SES-1318501.

- The role of gender in employees' self-reported cybersecurity behaviors is explored.
- Results show gender-wise differences for cybersecurity self-efficacy and behavior.
- Training is needed to close the gender gap in cybersecurity self-efficacy.