Securing Mobile Devices: Evaluating the Relationship between Risk Perception, Organisational Commitment and Information Security Awareness

A. Reeves[1], K. Parsons[2], and D. Calic[2]

[1]School of Psychology, University of Adelaide, South Australia
[2]Defence Science and Technology Group, Edinburgh, South Australia
e-mail: andrew.reeves@student.adelaide.edu.au; { dragana.calic; kathryn.parsons } @dst.defence.gov.au

Abstract

This study examined the relationship between perception of risk, organisational commitment, and Information Security Awareness (ISA). An online survey was completed by 269 working Australians. Perceptions of the Internet of Things (IoT) risk as it pertains to physically securing mobile devices was assessed. Organisational commitment and perception of personal risk significantly predicted ISA, as did two of the psychometric paradigm items. Demographic variables (age and gender) also significantly predicted variance in ISA, as did frequency of workplace information security training, albeit negatively. By identifying organisational commitment and perception of personal risk as significant predictors of ISA, this research has the potential to inform the development of information security training, aiming to enhance employee ISA.

Keywords

Risk perception; organisational commitment; Information security awareness (ISA); mobile devices; Internet of Things.

1. Introduction

Stable information security systems are critical for organisations to run effectively. Cyberthreats and their associated risks pose a significant threat to this stability. Employees have been found to be the most prevalent cause of information security breaches (PricewaterhouseCoopers 2015), with human error being implicated in 95% of security incidents (IBM Global Technology Services 2014). As a result, businesses are investing more resources into training programs designed to teach their staff how to identify and avoid these threats. For these training programs to be effective, it is crucial to understand the factors that influence an employee's behaviour in an information security context. Specifically, research needs to consider how businesses can encourage their employees to comply with the best-practice behaviours that are often outlined in the business's information security policy (ISP) (Arachchilage & Love 2014). The focus of this study is to examine the effect of risk perceptions and organisational commitment on Information Security Awareness (ISA). The following sections will introduce the main constructs considered in this study, namely, ISA, the psychometric paradigm of risk perception, perception of personal risk, and organisational commitment.

1.1. Information security awareness and the HAIS-Q

ISA is understood as the combination of a person's knowledge of, and attitude towards, best-practice information security behaviours, as well as their compliance with these behaviours (Parsons et al. 2014). To date, the most comprehensive, reliable and valid measure of ISA is the Human Aspects of Information Security Questionnaire (HAIS-Q) (McCormac et al. 2017; Parsons et al. 2013). The HAIS-Q examines seven focus areas, namely, password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting.

While the HAIS-Q has been extensively tested for reliability and validity (McCormac et al. 2017; Parsons et al. 2014; Pattinson et al. 2016), gaps in the literature still remain. There is a need to further assess the individual and organisational factors that may affect ISA (McCormac et al. 2017). For example, the relationship between ISA and other variables such as organisational commitment and risk perception have yet to be examined. Furthermore, the HAIS-Q has yet to be administered in relation to newly evolving threats (McCormac et al. 2017). The Internet of Things (IoT) has become a more recent focus of information security research, with the majority of cybersecurity professionals reporting concern regarding the risks of the IoT (ISACA 2016). IoT risks are unique, as IoT devices are often located outside of physically restricted areas (e.g., a restricted work building), but remain connected to the work network (Cisco 2015). Additionally, technical design of these devices is often lacking, resulting in inadequate security measures. Therefore, IoT devices are a potential entry point for an attacker. No study to date has assessed employees' perceptions of these risks in relation to ISA.

1.2. Perceptions of risk and the psychometric paradigm

There is a body of well-established research relating to people's perceptions of risk events (Sjöberg 2000; Sjöberg, et al. 2004; Slovic, et al. 1980a; Slovic et al. 1980b). Risk is defined as the probability of adverse effects and the magnitude of the consequences (Rayner & Cantor 1987). Slovic, et al. (1980b) identified eighteen risk perception constructs and demonstrated that these could be explained by two factors: dread and novelty. Dread refers to the extent to which someone is frightened, troubled, or generally retracts away from the risk, at the level of a gut reaction (Slovic, et al. 1980b). Novelty (also described as familiarity) refers to the extent to which someone feels they have knowledge and understanding of the risk, and how much control they have over it and its consequences. These two factors have explained the majority of variation in risk perception across 90 hazards. Since then, these results have been replicated in a variety of contexts (Bronfman, et al. 2008; Siegrist, et al. 2005; Sjöberg 2000). This framework is known as the psychometric paradigm.

The psychometric paradigm has only once been applied to information security risks. Huang, et al. (2010) found support for many of the same risk perception constructs identified by Slovic, et al. (1980b). However, they did not find support for the two factor structure, dread and novelty. This was likely due to methodological limitations. For example, the 602 participants responded to only one of the twenty-one threats examined in the study. This meant that each threat was only examined by a small number of people (as few as 23). In addition, the two factor structure developed by Slovic, et al. (1980b) has been extensively validated, improved and replicated (Sjöberg 2000; Sjöberg, et al. 2004; Slovic, et al. 1980a; Slovic et al. 1980b), whereas there is no additional support for the structure found by Huang, et al. (2010). These limitations indicate that further research is required into the application of the psychometric paradigm to information security.

1.3. Perception of personal risk

To capture information security risk perceptions at a more concrete level, Pattinson and Jerram (2013) investigated the risk perceptions of employees from a government organisation. Using the Repertory Grid Technique, the authors elicited 110 constructs relating to information security risk perceptions. These constructs were categorised into five themes: Risk perceptions relating to my organisation; risk perceptions relating to me; risk perceptions relating to others; why I think it's a risk; and, miscellaneous. Of interest here is the 'risk perceptions relating to me' theme, as it contains 11 personal risks perceived by the employee, such as fear of reprimand and loss of personal data. Intuitively, employees who perceived business risks as personal should actively avoid the behaviours that lead to those events, and thereby have greater ISA. However, this has yet to be examined empirically.

1.4. Organisational commitment

Organisational commitment relates to how attached an employee is to their place of work. An employee who is greatly attached and committed to their workplace should work harder, strive to make fewer mistakes, and follow organisational policy diligently (Mowday, et al. 1979). Therefore, more committed employees should have better ISA. Meyer and Allen (1991) purport that organisational commitment is a combination of the affective, normative, and continuance factors that influence an employee's decision to remain in their organisation. The affective factor refers to the emotional aspects of commitment. The normative component refers to the extent to which an employee feels that remaining at one organisation is expected by society, or is morally right. The continuance component refers to the more pragmatic reasons an employee might wish to remain with an organisation, such as the difficulty of finding new work and the cost of moving organisations. Organisational commitment has been found to be a small, significant predictor of job performance (Riketta 2002). Although previous research has considered the relationship between organisational commitment and ISA, it lacked a validated measure of ISA (e.g., Stanton et al. 2003).

1.5. Study aims and hypotheses

This study aims to investigate the extent to which an individual's commitment to their organisation and perception of information security risks relate to their ISA. Organisational commitment, perceived personal risk, the psychometric paradigm of risk perception, and ISA were measured as they pertain to the risk of mobile computing. It is hypothesised that people who have a greater perception of risk and more commitment to their organisation will have greater ISA. As age, gender, and other individual difference variables have been shown to be significant predictors of ISA (McCormac et al. 2017), their effect on ISA will also be examined.

2. Methodology

Data collection consisted of an online survey, administered through Qualtrics. The Human Research Ethics Subcommittee of the University of Adelaide, School of Psychology, granted ethics approval. The data collected for this paper formed part of a larger project. For this paper, data analysis will focus on responses obtained from the demographic questions (e.g., age, gender), the results from the HAIS-Q: Mobile Devices, and perception of personal risk scales, as well as responses to the organisational commitment and psychometric paradigm questionnaires.

2.1. Participants

A total of 269 participants responded to the online questionnaire (144 male, 125 female). Participants were recruited through researchers' Facebook pages, and a closed invitation-only panel recruitment method via Qualtrics. Participants were required to be employed in Australia, and be over the age of 18. Participants were well distributed in terms of age, with the largest group being between 30 and 39 years of age (37%). Approximately 22% of participants were between 18 and 29 years of age, 20% were 40 to 49 years of age, leaving 14% in the 50 to 59 age category, and 7% in the 60 and above age category. Participants were employed in a range of industry sectors including trade, finance, education, and manufacturing, and included managers (42%), team leaders (13%), and regular staff (45%).

2.2. Materials

The survey consisted of following measures, each scored on a 5-point Likert scale (1 = strongly disagree to 5 = strongly agree).

2.2.1. HAIS-Q: Mobile Devices

This sub-scale measures information security awareness relating to mobile devices (Parsons et al., 2017). The measure consists of 9 items. Cronbach's alpha was .81 which is consistent with previous research (Parsons et al., 2017).

2.2.2. Organisational Commitment Questionnaire

This scale measures the affective, normative, and continuance components of commitment to an organisation (Meyer & Allen 1991). The scale contains 24 items. Cronbach's alpha was .82 which is consistent with previous literature (Meyer & Allen, 1991).

2.2.3. Perception of Personal Risk (PPR) Scale

This scale, developed for this study, measures how personally at-risk individuals feel in relation to the threat to information security posed by mobile computing. Participants were provided with a description of the mobile computing threat posed by the theft of a laptop as an IoT-related risk (See Appendix A). This was followed by 11 items relating to personal risk (adapted from Pattinson and Jerram (2013)). Participants were required to rate the perceived likelihood and severity of consequences for each of the 11 items. Cronbach's alpha score for this scale was .95.

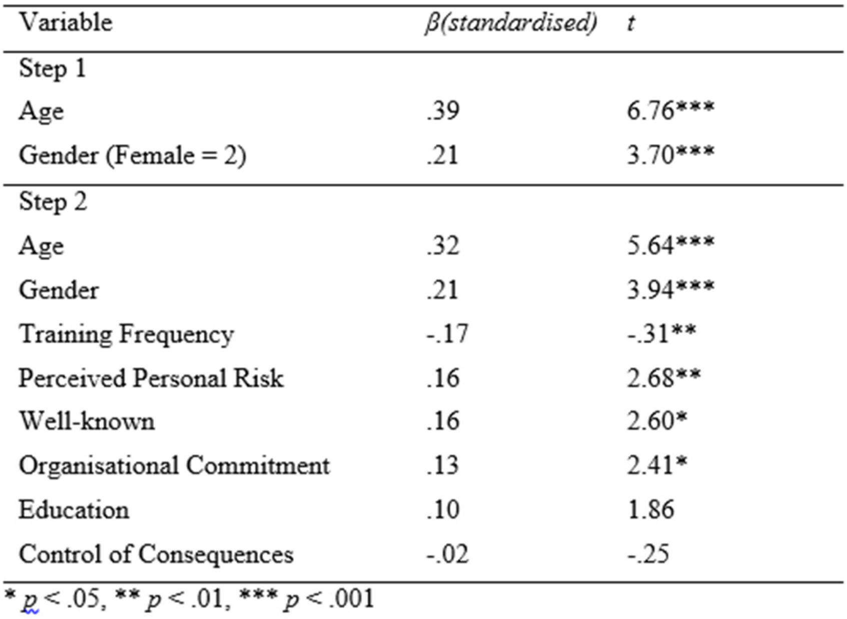
2.2.4. Psychometric Paradigm Risk-Perception Items

The psychometric paradigm can be used to measure participants' perception of risk in relation to two factors: dread and novelty (Slovic, et al. 1980b). In this study, dread was measured using the items 'dreaded' and 'control of consequences' and novelty was measured using the items 'immediacy of consequences' and 'well known'. Participants responded in relation to the threat posed by the theft of a laptop for each item.

3. Results

Pearson bivariate correlations were examined between ISA, gender, age, education, information security training frequency, knowledge of computers, organisational commitment, perceived personal risk, and the psychometric paradigm items. As shown in Appendix B, the correlations between ISA and knowledge of computers, as well as two of the psychometric paradigm items (i.e., dreaded and immediacy of consequences), were not significant, and are not considered in the following regression. To ensure multicollinearity had not occurred, Variance Inflation Factor (VIF) values were calculated, and all were below 2.

As shown in Table 1, a hierarchical multiple regression was conducted to test the extent to which demographic variables, perceived personal risk, organisational commitment, and the psychometric paradigm items predicted ISA. As age and gender are well established predictors of ISA (McCormac et al. 2017), they were entered in step one to control for their effects. Both age and gender were significant, together explaining approximately 18% of the variance in ISA ($F(2, 266) = 29.6$, $p < .001$). Added in step two were perceived personal risk, organisational commitment, the two psychometric paradigm items (i.e., 'Well-known' and 'Control of Consequences'), and the two remaining demographics (i.e., education and information security training frequency). The model at step two explained approximately 32% of the variance ($F(8, 260) = 15.1$, $p < .001$). All but two predictors were significant: the psychometric paradigm item: ‘Control of Consequences’ (p = .801); and, education (p = .064). The most important predictors were, in order from greatest to least: age, gender, information security training frequency, perceived personal risk, the ‘well-known’ psychometric paradigm item, and organisational commitment.



Variable	*β(standardised)*	*t*
Step 1		
Age	.39	6.76***
Gender (Female = 2)	.21	3.70***
Step 2		
Age	.32	5.64***
Gender	.21	3.94***
Training Frequency	-.17	-.31**
Perceived Personal Risk	.16	2.68**
Well-known	.16	2.60*
Organisational Commitment	.13	2.41*
Education	.10	1.86
Control of Consequences	-.02	-.25

* $p < .05$, ** $p < .01$, *** $p < .001$

Table 1: Summary of hierarchical multiple regression of independent variables predicting ISA (N = 269)

4. Discussion

While there is ample research investigating organisational commitment in relation to job performance (Cohen 1993; Porter et al. 1974; Riketta 2002), there is limited research looking at its influence on ISA. Likewise, there exists a body of research regarding risk perceptions (Sjöberg 2000, 2003; Slovic, et al. 1980a; Slovic et al. 1980b); however, its application to information security contexts is lacking. Finally, personal risk perceptions have been identified as important in this context (Pattinson & Jerram 2013), but have not been considered in relation to ISA. In addition, newly evolving risks in relation to IoT have not been considered previously. Therefore, the present study examines these relationships, by applying measures of these constructs to a single cohort in the context of an IoT risk. Employees who were more committed to their organisation had higher ISA scores. Likewise, participants who perceived the risk as more well-known or more personal had higher ISA. Lastly, participants’ age, gender, and frequency of information security training all predicted ISA.

In line with previous findings (e.g., McCormac et al. (2017)), age and gender were significant predictors of ISA in this study. ISA improved with age and females had higher scores than males. This has important implications for information security training programs. Interestingly, while it did correlate with ISA, education did not predict significant variance. As the result was close to significance, the lack of significance may be due to the relatively small sample size. Studies with larger cohorts may be able to detect the effect of education on ISA. That said, the size of the effect is small, indicating the influence of education on ISA may not be important. While it may seem intuitive for information security training programs to be targeted at less educated employees, this finding would question that assumption.

Employees who reported more frequent information security training at work had lower ISA. This is somewhat in keeping with previous research, which has found that employees who have undertaken formal information security training have lower ISA, perhaps due to overconfidence and complacency (Parsons et al. 2013; Pattinson et al. 2015; Pattinson et al. 2016). However, in previous research this only applied to external training. Training conducted within an organisation was found to lead to higher ISA (Pattinson et al. 2016). The findings of the current study contradict this, as greater internal training frequency was associated with poorer ISA. This finding highlights the importance of organisations gearing information security training in such a way as to avoid instilling overconfidence or complacency in their staff. Furthermore, it is critical for businesses to measure the ISA of their staff, using a measure such as the HAIS-Q, before and after the training program, to ensure the intervention was successful.

A similarly counter-intuitive result was found regarding familiarity with computers, which had no significant relationship with ISA. This conflicts with previous research, which has found, also counter-intuitively, that people less familiar with computers may have greater ISA (Pattinson et al. 2015). This inconsistency may point to the relative unimportance of familiarity with technology in information security contexts. That said, participants who reported being more familiar with the information security risk itself had higher ISA scores. Businesses should focus on effective training to increase employee familiarity with information security risks, as having staff who are highly experienced with technology in general is not sufficient to ensure cybersecurity.

Greater organisational commitment was also associated with greater ISA scores, despite it being the smallest significant predictor. This supports the results of previous studies which have looked at the relationship between organisational commitment and ISA, but lacked a validated ISA measure (Stanton et al. 2003).

As expected, participants who perceived the information security risk as personal had greater ISA. This indicates that, in the case of mobile computing/IoT risks, employees who feel personally at risk (e.g., of reprimand, reduced productivity, personal data loss) are more likely to avoid behaviours that may lead to the risk event occurring, resulting in greater ISA. Training programs that focus on informing staff of the risks of mobile computing/IoT should highlight where the employee may be at-risk should the event occur, in order to encourage better ISA.

4.1. Limitations and future directions

The data reported in this paper focused on only one information security risk: mobile computing/IoT. The relationships discovered may differ in regard to other information security risks, and this should be examined in future research. A future paper will report on two other information security threats, phishing and malware. In addition, the measure used to assess perception of personal risk was developed for this study. While the items used have been found to be important in understanding employee cybersecurity risk perceptions (Pattinson & Jerram 2013), its use as a measure has not yet been empirically validated. That said, the findings of this study provide preliminary support for its use. Lastly, there is an opportunity for further analysis to be performed on the data, such as hierarchical clustering or principle component analysis. While this is outside of the scope of the present paper, a future paper may present this analysis.

4.2. Conclusion

This study examined the relationship between organisational commitment, perception of personal risk, and ISA. More highly committed people had better ISA, as did people who more greatly perceived the risk as personal. This finding has important implications for information security training programs, which in the case of mobile computing and IoT risks should focus on where the employee is potentially at-risk. Businesses should also look to cultivate organisational commitment in their staff, in order to encourage better ISA.

5. References

Arachchilage, N & Love, S 2014, 'Security awareness of computer users: A phishing threat avoidance perspective', *Computers in Human Behavior*, vol. 38, pp. 304-312.

Bronfman, NC, Cifuentes, LA & Gutiérrez, VV 2008, 'Participant-focused analysis: explanatory power of the classic psychometric paradigm in risk perception', *Journal of Risk Research*, vol. 11, no. 6, pp. 735-753.

Cisco 2015, *The Internet of Things: Reduce Security Risks with Automated Policies*, https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf, (Accessed 8 August 2017)

Cohen, A 1993, 'Organizational Commitment and Turnover: A Meta-Analysis', *The Academy of Management Journal*, vol. 36, no. 5, pp. 1140-1157.

Huang, D-L, Rau, P-LP & Salvendy, G 2010, 'Perception of information security', *Behaviour & Information Technology*, vol. 29, no. 3, pp. 221-232.

IBM Global Technology Services 2014, *IBM security services 2014 cyber security intelligence index*. https://www.ibm.com/developerworks/library/se-cyberindex2014/index.html, (Accessed 1 August 2017).

ISACA 2016, *State of cybersecurity: implications for 2016. An ISACA and RSA conference survey. http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf, (Accessed 10 August 2017)*

McCormac, A, Zwaans, T, Parsons, K, Calic, D, Butavicius, M & Pattinson, M 2017, 'Individual differences and Information Security Awareness', *Computers in Human Behavior*, vol. 69, pp. 151-156.

Meyer, JP & Allen, NJ 1991, 'A three-component conceptualization of organizational commitment', *Human Resource Management Review*, vol. 1, no. 1, pp. 61-89.

Mowday, RT, Steers, RM & Porter, LW 1979, 'The measurement of organizational commitment', *Journal of Vocational Behavior*, vol. 14, no. 2, pp. 224-247.

Parsons, K, McCormac, A, Butavicius, M, Pattinson, M & Jerram, C 2014, 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, vol. 42, pp. 165-176.

Parsons, K, McCormac, A, Pattinson, M, Butavicius, M & Jerram, C 2013, 'Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails', in *Security and Privacy Protection in Information Processing Systems (SEC),* Aukland, New Zealand.

Pattinson, M, Butavicius, M, Parsons, K, McCormac, A & Calic, D 2015, 'Factors that Influence Information Security Behavior: An Australian Web-Based Study', in T Tryfonas & I Askoxylakis (eds), *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings*, Springer International Publishing, Cham, pp. 231-241.

Pattinson, M, Butavicius, M, Parsons, K, McCormac, A, Calic, D & Jerram, C 2016, 'The Information Security Awareness of Bank Employees', in *Human Aspects of Information Security & Assurance (HAISA 2016),* Melbourne, Australia.

Pattinson, M & Jerram, C 2013, 'A study of Information Security Risk Perceptions at a Local Government Organisation', in *Australasian Conference on Information Systems,* Melbourne, Australia.

Porter, LW, Steers, RM, Mowday, RT & Boulian, PV 1974, 'Organizational commitment, job satisfaction, and turnover among psychiatric technicians', *Journal of Applied Psychology*, vol. 59, no. 5, pp. 603-609.

PricewaterhouseCoopers 2015, *Key findings from the global state of information security survey 2016. Turnaround and transformation in cyber security.*

Rayner, S & Cantor, R 1987, 'How Fair Is Safe Enough? The Cultural Approach to Societal Technology Choice1', *Risk Analysis*, vol. 7, no. 1, pp. 3-9.

Riketta, M 2002, 'Attitudinal organizational commitment and job performance: a meta-analysis', *Journal of Organizational Behavior*, vol. 23, no. 3, pp. 257-266.

Siegrist, M, Keller, C & Kiers, HAL 2005, 'A New Look at the Psychometric Paradigm of Perception of Hazards', *Risk Analysis*, vol. 25, no. 1, pp. 211-222.

Sjöberg, L 2000, 'Factors in Risk Perception', *Risk Analysis*, vol. 20, no. 1, pp. 1-12.

Sjöberg, L 2003, 'The Different Dynamics of Personal and General Risk', *Risk Management*, vol. 5, no. 3, pp. 19-34.

Sjöberg, L, Moen, B-E & Rundmo, T 2004, *Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research*, Trondheim, Norway.

Slovic, P, Fischhoff, B & Lichtenstein, S 1980a, 'Facts and Fears: Societal Perception of Risk', *Advances in Consumer Research*, vol. 8, p. 497.

Slovic, P, Fischhoff, B & Lichtenstein, S 1980b, 'Facts and Fears: Understanding Perceived Risk', in RC Schwing & WA Albers (eds), *Societal Risk Assessment: How Safe is Safe Enough?*, Springer US, Boston, MA, pp. 181-216.

Stanton, JM, Stam, KR, Guzman, I & Caledra, C 2003, 'Examining the linkage between organizational commitment and information security', in *IEEE International Conference on Systems, Man and Cybernetics, 2003.,* vol. 3, pp. 2501-2506 vol.2503.

Appendix A: Measure for Perception of Personal Risk

Definition: The 'Internet of Things' (IoT) refers to a network of internet-connected devices, including laptops, smartphones, and smart-appliances. In organisations, IoT devices are often located outside of physically restricted areas, but remain connected to the organisation's central network. Each IoT device therefore becomes a potential point of entry for an attacker, allowing them access to sensitive information on the organisation's network. *Instructions: You leave a work-connected device (e.g., Laptop, tablet, smart phone) unattended in a public place, and it is stolen. Please rate the likelihood & severity of the following (5-pt Likert):*	
I am reprimanded	*I am demoted*
I am fired	*My personal information is damaged/destroyed/leaked*
I can't do my job properly	*It is an inconvenience/time-consuming/nuisance*
My professionalism/quality of my work is tarnished	*It causes me stress*
I am required to take action and fix the problem	*My workload will increase*
I lose confidence in the information or systems required for me to do my job	

Appendix B: *Correlations, means and standard deviations (N = 269)*

Variables	1	2	3	4	5	6	7	8	9	10	11	12
1. Mobile-devices ISA												
2. Perceived Personal Risk	.25**											
3. Well-Known	.32**	.39**										
4. Dreaded	-.11	-.17**	-.41**									
5. Immediacy of Consequences	-.11	-.18**	-.30**	.16**								
6. Control of Consequences	-.16**	-.37**	-.36**	.14*	.36**							
7. Organisational Commitment	.26**	.18**	.25**	-.06	-.03	-.14*						
8. Age	.37**	.05	.25**	-.11	-.10	-.11	.16**					
9. Gender	.18**	-.03	-.05	.15*	-.03	-.04	.04	-.07				
10. Education	.15*	.07	.08	-.09	-.06	-.13*	.01	.04	.02			
11. Information Security Training Frequency	-.16**	.12	.15*	-.10	-.10	-.02	.08	-.19**	-.06	-.06		
12. Knowledge of Computers	.06	.10	.23**	-.09	-.09	.00	.08	-10	-.16**	-.05	.19**	
Mean	36.2	126.8	3.7	3.3	3.4	3.6	78.1	^	^	^	^	^
SD	6.4	62.1	1.1	1.2	1.2	1.0	12.2	^	^	^	^	^

* $p < .05$ (2-tailed) ** $p < .01$ (2-tailed) ^ Mean and SD values are unavailable, as ranges rather than exact values were provided by participants.