International Journal of Cyber Criminology
Vol 12 Issue 1 January – June 2018

Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom

Lee Hadlington[1]
De Montfort University, United Kingdom

Abstract

The present study aimed to explore if the size of company an individual works for, age or attitudes towards cyber security affected frequency to engage in risky online behaviours. A total of 515 participants aged between 18-84 in full or part-time employment were asked to complete a questionnaire that consisted of two scales. One measured their attitude towards cyber security and general awareness of cyber crime, the other examined the types of 'risky' cyber security behaviours they were engaged in. The results demonstrated a significant negative correlation between attitudes towards cyber security and risky cyber security behaviours, with more negative attitudes being linked to higher levels of risky behaviours. There were also significant differences according to company size and age group according to frequency of engaging in risky cyber security behaviour and attitudes towards cyber security. The findings are presented as furthering our understanding of how employee attitudes contribute to company cyber security, as well as highlighting how the size of an organisation could be linked to difference in knowledge and adherence to ISA protocols.

Keywords: Accidental insider, risky cyber security behaviours, cyber security, Information security.

Introduction

In the fight to protect organisations from information theft and cyber crime, a great deal of attention has been devoted to improving existing information security infrastructure (Herath & Rao, 2009a, b). The focus on technical solutions to cyber security often fails to acknowledge that for such systems to be effective, employee engagement and understanding of their utility is required (Sasse & Flechais, 2005). A number of researchers have commented on the realisation that, for the most part, the weakest element in the cyber security chain is that of the human (Anwar et al., 2016; Herath & Rao, 2009b). Aspects of passive engagement, lack of knowledge, misdirected attention and engaging in *risky* cyber security behaviours all have the potential to increase organisational susceptibility to security flaws (Sasse & Flechais, 2005). Having a deeper understanding of how individual differences related to employee adherence to IT security

[1] Senior Lecturer, Psychology Division, De Montfort University, The Gateway, Leicester, LE1 9BH, UK. Email: lhadlington@dmu.ac.uk

protocols could hold the key to managing an effective cyber security posture within an organisation. In a similar context, exploring how organisational factors such as the size of the company for which the individual works could also provide another metric for isolating those companies that might have a higher risk of being victimized due to a breach in cyber security. The present study aims to explore if there are significant differences in employees engaging in risky cyber security behaviours based on their age, the size of the company, or the employee's attitudes towards cyber security and cyber crime.

Exploring the threat from within the Organisation

Over the past decade there has been an increasing amount of attention directed towards exploring aspects of *insider threat*. The insider threat is typically defined as a current or former employee who has (or had) access to internal systems, and through this access they are able to conduct a variety of malicious activities (Claycomb, Huth, & Flynn, 2012). The threat from insider has been presented as a growing concern for the internal security of an organisation(Claycomb et al., 2012; Greitzer, Kangas, Noonan, & Dalton, 2010; Keeney, 2005; Probst, Hunker, Gollmann, & Bishop, 2010). The threat from the insider is multifaceted and relates in part to breaches in security, impact on the prestige of the company, and related financial loss (CPNI, 2013).

The focus for insider threat is often on incidents where aspects of intentionality or motive are central; therefore threats from unintentional actions are often overlooked. However other researchers have argued against the label of *insider threat* and adopted the more flexible term of *insiderness* (Bishop, Gollmann, Hunker, & Probst, 2008; Hunker & Probst, 2011). For example, Hunker and Probst (2011) presented a comparison of the actions for *accidental insiders* to those of a *real insider*, the latter being a category where individuals exhibit malicious intent in their exploits and advanced skills or expertise, including knowledge related to programming, IT infrastructure and company systems. At the opposite end of the continuum are the *accidental* or *unintentional* insiders. These are individuals who have limited knowledge of accepted security protocols, their actions are obvious, and they make no direct attempt to cover up their mistakes. It is the accidental insiders who present the focus for this current work, alongside an examination of how individual differences could make certain people more prone to lapses in cyber security. The CERT (2013) report presented a very detail definition of the unintentional insider threat (UIT), which is:

> … a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. (CERT, 2013, p. ix)

This definition focuses directly on threat as a result of inaction or specific lack of knowledge and also highlights the lack intent to cause harm. The key components for the conceptualization of UIT are directly linked to human failure and limitations in human performance (CERT, 2013). These mistakes include those made though job-related time pressures, task difficulty, a lack of knowledge, and cognitive factors such as inattention

(CERT, 2013). Examples of UIT presented by CERT (2013) included accidental disclosure of sensitive information (either via website, email or fax); devolving of log-in details (password and username) either as a result social engineering or via malware/spyware; the improper disposal of physical records; the loss of information through the misplacement of smart-phones, USB drives, DVDs, CDs and hard drives. These random acts present a greater concern for organisations as they have no motive, no intent and no prior indicators upon which to act. Unfortunately, the end result is still the same, and the actions of the UIT can be as damaging as those perpetrated by the malicious attacker.

Examining Individual Differences in Cyber Security

In the context of UIT, some researchers have explored information security behaviours alongside an examination of psychological constructs such as personality traits. Egelman and Peer (2015a; 2015b) presented the development of the Security Behaviours Intentions Scale (SeBIS), designed to explore an individual's adherence to computer security advice. Egelman and Peer (2015b) noted individuals scoring higher on measures of inquisitiveness were more likely to engage in better security practices. Good security practices were also linked to an assessment of the long-term impact for the individuals' current actions. Personality constructs such as impulsivity were negatively associated with adherent cyber security behaviours. Research from Egelman and Peer (2016b) suggested that those individuals who are quick to react or fail to think carefully about their decisions (such as responding quickly to a phishing email) are less engaged in good cyber security behaviours. Those individuals who demonstrated a capacity to engage proactively in decision-making also scored higher on the SeBIS showing that active cyber security is not associated with a reliance on others (Egelman and Peer, 2015b).

Previous work has also examined the link between age of individuals and their adherence to information security protocols. For example (McCormac et al., 2017) found that older adults (30-65+ years) had higher scores on a measure of information security awareness compared to younger adults (18-29 years). They also noted that such a relationship was linear in nature, with information security scores increasing with the age of the participant. Previous research by Sheng et al. (2010)had also noted that those individuals aged between 18-25 were more likely to fall for phishing attacks versus any other age group. According to these researchers this group tends to be more susceptible to phishing attacks as they have a lower level of education, have spent fewer years on the Internet and also have had less exposure to relevant training materials(Sheng et al., 2010). They also noted that this age group were less risk averse compared to the older participants in their study, a finding which also fits into previous research linking age to risky behaviours (Reyna & Farley, 2006).

However, the link between age and risky cyber security behaviours is still limited to just a handful of studies. In the context of the present study the concept of risky cyber security behaviours is viewed as any activity that places the individual and organisation at increased threat from malicious attacks (Hadlington, 2017; Hadlington & Parsons, 2017). Such activities can include sharing personal passwords, downloading copyrighted material from illegal websites and ignoring warnings to update apps and computer software. A further exploration of the way in which age impacts on both attitudes towards cyber security and engagement in risky behaviours could have clear practical uses, particularly

when it comes to designing effective communication packages for cyber security awareness.

Aims and Objectives of the Present Study

The notion of UIT presents a potential starting point from which researchers, the police and security professionals can explore non-malicious threats within an organisation. There is still a limited amount of empirical research that directly examines how individual differences could serve to influence the potential for UIT, perhaps due to the belief that technical solutions can provide mitigation for such. The aim of the present study is to explore if the frequency of engaging in risky cyber security behaviours can be linked to organisational factors (size of organisation for which the individual works for), their age, and their attitudes towards cyber security. Previous work has noted that the size of an organisation can influence key aspects of cyber security, including aspects related to training and budgetary commitments (Briney & Prince, 2002; Osborn, 2015). Exploring the role company size has upon engagement in risky cyber security behaviours and employee attitudes towards cyber security could provide another important metric to help target awareness in a more proactive way. Therefore the aims of the present study are captured in the following hypotheses:

> *H1: There will be a significant difference between age groups and company size based on respondent's attitudes towards cyber security.*
>
> *H2: There will be a significant difference between age groups and company size based on respondent's engagement in risky cyber security behaviours.*

Method

Participants

Participants were recruited via an online questionnaire through Qualtrics Online Sampling between 15th-20th October 2016, and were paid a small honorarium of £3 for their participation. In total 538 participants completed the survey, all of which were based in the U.K. Data from 23 respondents were deleted and excluded from further analyses due to incomplete or missing data.

The final dataset included 515 participants, comprising of 218 Males and 297 Females. For the sample of 515 participants, the participants had an age range of 18 – 84, (18-24 = 17%, 25-34 = 30%, 35-44 = 3%, 45-54 = 24%, 55-64 = 24%, 65+ = 3%). For the purposes of the ANOVA analysis, two age groups with roughly equal numbers in each were created (18-34 and 35-64+) based on the findings from McCormac et al. (2017). All participants were in employed, with the majority of respondents (70%) being full-time, and the remainder (30%) being part-time. In terms of company size, 12% of respondents worked for organizations with less than 10 employees, 21% with 11-50 employees, 22% with 51-250 employees and 44% worked for companies with more than 250 employees.

Measures

a. Risky cyber security behaviours scale (RScB)

Hadlington (2017) presented the development of a scale designed to explore key activities that could potentially lead to individuals being compromised as a consequence of poor cyber security practices. Participants are asked to rate on a 5-point Likert scale (*0=Never - 5 = Daily*) how often they engaged in the specific behaviour during a one-month period. Items included '*sharing passwords with friends and colleagues*' and '*Using the same password for multiple websites*'. A Cronbach's alpha of .823 was obtained for the full 20-item scale, indicating good internal reliability. Possible scores on the RScB can range from 0-100. Higher scores on the RScB were indicative of the individual engaging in more risky online behaviours.

b. Attitudes towards cyber security in business (ATC-IB)

This scale examines attitudes related cyber security as well as examining how individual employees perceived the threats from cyber crime (Hadlington, 2017). Aspects included responsibility for cyber security in the organization, perceived effectiveness of the Police in dealing with cyber crime, signposting of relevant information, and engagement with cyber security awareness.

The scale consists of 25 items and includes questions such as *I don't have the right skills to be able to protect the organization from cyber crime* and *I do not feel that IT security is a priority within my organization*. The scale is scored using a 4-point Likert scale (1=Strongly Agree – 4 = Strongly Disagree). A high score on the ATC-IB scale indicates positive engagement and awareness in cyber security; where as a lower score indicates poorer engagement and limited awareness. Scores on the ATC-IB can range from 25 – 100. A Cronbach's Alpha of .764 was achieved in the current study indicating good internal reliability.

Results

Means and standard deviations for the RScB and ATC-IB as a function of age and company size are presented in Tables 1 and 2. The responses to the items from the ATC-IB are presented in Table 3.

Table 1. Means and Standard Deviations for total scores on the Risky Cyber security Behaviours Scale (RScB) according to age and company size

Variable	*M*	*SD*	*n*
Age Group			
18-34	28.55	15.99	242
35-64	19.44	12.23	273
Total	23.72	14.81	515
Company Size			
10 or less	23.17	16.38	63
11-50	25.61	14.96	110
51-250	27.07	17.97	115
250 +	21.25	11.85	227
Total	23.72	14.81	515

Table 2. Means and Standard Deviations for total scores in the Attitudes towards Cyber security in Business (ATC-IB) according to age and company size

Variable	M	SD	N
Age Group			
18-34	58.55	7.30	242
35-64+	61.65	7.02	273
Total	60.19	7.312	515
Company Size			
10 or less	59.77	8.37	63
11-50	59.04	6.20	110
51-250	59.18	7.31	115
250 +	61.38	7.37	227
Total	60.19	7.31	515

Table 3. Scale items from the ATC-IB[2] & responses (%)

	Item	Strongly Agree	Agree	Disagree	Strongly Disagree
1	I think that management have the responsibility to ensure a company is protected from cyber crime	53	44.5	1.7	0.8
2*	I am aware of my role in keeping the company protected from potential cyber criminals.	2.5	10.7	54.0	32.8
3	I believe everyone in the company has a role to play in protecting against threats from cyber criminals.	42.9	50.5	5.2	1.4
4	It is hard to know how I can help protect the organisation from cyber crime.	8.5	50.1	35.9	5.4
5	I don't have the right skills to be able to protect the organisation from cyber crime.	9.7	46.2	38.6	5.4
6	I do not feel that IT security is a priority within my organisation.	5.4	28.9	43.5	22.1
7	Computer systems provide all the protection a company needs.	7.0	29.0	52.0	12.0
8	I think that reporting cyber crime is a waste of time.	2.1	15.3	51.1	31.5
9	The Police lack the capacity to deal with cyber crime effectively.	10.1	53.6	32.4	3.9

[2] (from Hadlington, 2017)

10	I believe that cyber criminals are more advanced than the people who are supposed to be protecting us.	18.6	60.2	19.8	1.4
11	I think that information provided by the Government and Police on cyber crime is not relevant to businesses.	4.9	31.1	56.9	7.2
12	I feel that the Police are far too busy to deal with cyber crime.	13.0	53.0	30.7	3.3
13	I worry that if I report a cyber attack to the Police it might damage the reputation of the company	5.0	29.7	54.2	11.1
14 ⋆	I think more could be done to communicate the risks from cyber crime to individuals in the organisation.	1.6	12.8	70.1	15.5
15 ⋆	I am aware of the company's IT use policy and attempt to follow it.	2.7	15.5	55.7	26.0
16	I would not know how to report a cyber attack if one happened.	8.3	35.5	44.3	11.8
17	I don't think that reporting a cyber attack on the company is my responsibility.	5.6	44.3	41.9	5.8
18	I don't pay attention to company material about the threats from cyber crime.	2.9	21.9	56.1	19.0
19 ⋆	I am confident that I would be able to spot the signs of a cyber attack.	6.4	43.5	44.3	5.8
20 ⋆	I think the biggest threat for IT systems comes from people within the company.	5.6	44.3	41.9	8.2
21 ⋆	I feel that any individual within the company are at risk of manipulation from confidence tricksters.	1.4	16.5	65.2	16.9
22	I think that cyber criminals only target a company when there is a substantial financial gain.	9.5	39.4	43.9	7.2
23	I believe that only large companies are targeted by hackers and cyber criminals.	4.3	19.8	60.6	15.3
24	I feel that only companies that take payments using online systems are at risk of being victims of cyber crime.	7.4	25.3	52.4	14.8
25	I don't think I know who is responsible for protecting the company from cyber crime.	6.6	42.3	40.2	10.9

⋆ = indicates a reversed score item

A correlation revealed a significant negative correlation for total scores on the RCsB questionnaire and total scores on the ATC-IB (r = -.302 (515), p = .000), suggesting that a more positive attitude towards cyber security is linked to a decrease in the frequency with which they engage in risky cyber security behaviours. In the following section the scores for both the RScB and ATC-IB are reported in terms of age group differences and company size for which the individual is working.

i. Age, Company size and Risky Cyber security Behaviours

A one-way between subjects ANOVA revealed a significant difference between age groups and scores on the RScB F (*1, 513*) = 53.392, p = 000, η_p^2 .094, indicating a medium effect size. A further between subjects ANOVA revealed a significant main effect for company size and scores on the RScB, F (3, 511) = 4.790, p> .005, η_p^2 .027 indicating a small effect size. Further post hoc comparisons revealed significant differences between those employed by companies over 250 employees and those with between 51-250 employees (p> .005).

ii. Age, Company Size and Attitude towards Cyber security

A between subjects ANOVA revealed a significant difference between age groups and scores on the attitudes towards cyber security in business scale F (*1, 513*) = 24.134, p = 000, η_p^2 = 0.045, indicating a medium effect size.

A further between-subjects ANOVA revealed a significant main effect for company size on attitudes towards cyber security, F(3, 511) = 3.783, p= 0.11, η_p^2 = 0.022, indicative of a medium effect size. A post hoc comparison showed a significant difference between overall scores on the attitude scale for employees in companies over 250 + and 51-250 (p= 0.50) and for 250+ and 11-50 employees (p = .033).

Discussion

The present study aimed to provide empirical evidence examining how aspects of age, individual differences in attitudes towards cyber security, and company size impact on the cyber security posture of an organisation. The results supported the hypotheses for the study, as there were significant differences according to both age and company size in relation to the frequency with which individuals engaged in risky cyber security behaviours.

1. Attitudes towards Cyber security

One of the fundamental findings from exploring the attitudes of employees is the apparent sense of devolved responsibility they have in terms of their cyber security responsibilities within an organisation. This would potentially align with suggestions from Tischer et al. (2016) that individuals are devolving a responsibility for their cyber security to technical interventions and senior management. The attitude appears to be that once they are in their place of employment they no longer see cyber security as their primary concern. This would also fit into a risk compensation framework, where an individual who believes they are protected by technical interventions provided by their host organisation may in turn engage in more risky cyber security behaviours (Hadlington & Parsons, 2017).

Many participants expressed a lack of knowledge or skill related to being able to deal with cyber security incidents. Fifty-eight per cent of those questioned claimed that they did not to know how to protect the company from cyber crime. An additional 55% reported that they thought they did not have the skills necessary to fulfil this responsibility (see Table 3). This may reflect a belief that specialist knowledge or skills such as programming proficiency or digital forensics are needed to be able to actively engage in cyber security. As a future piece of research, it would be useful to examine this aspect further and identify what specific skills employees believe they need in order to be engaged in this role.

Issues related to a lack of attention to information and awareness related to key risks is also highlighted, where 84% of respondents appeared to feel that there is already enough information about communicating the key risks from cyber crime. It could be that individuals face an inordinate amount of material related to potential risks that could be leading to less attention being paid to them. This is in part evidenced by an additional 25% of respondents who admitted to regularly ignoring information from employers communicating current threats and how to prevent them. It would again be useful to explore the reasons why individuals choose to ignore such information in future research. As noted by Egelman and Peer (2015), end users are often presented with messages about cyber security that are both inconclusive and inconsistent, so ignoring these messages could be a more effective use of their time. Indeed, Egelman, Cranor, and Hong (2008) had shown that where less-frequent high-risk warnings appeared in a similar way to frequent low-risk security warning, this had the effect of leading end users to actively ignore both.

A high percentage of those who responded viewed the police to be ineffectual when it comes to dealing with cyber crime. Overall, 80% of respondents believed that cyber criminals were more advanced than those who were preventing the attacks. When exploring their capacity to deal with cyber crime effectively, 66% viewed the police as having clear limitations. Contrary to this, only 17% of respondents saw reporting cyber crime as a waste of time; however, there is no additional data to explore if participants knew exactly where to report such events. These finding are problematic from a number of perspectives. If individuals believe that the police are ill equipped to deal with cyber crime, they may in turn believe reporting such incidents to be ineffectual and pointless. Further research should explore the potential reasons as to why individuals hold such attitudes, as such beliefs could have a clear impact on the potential for the under reporting of cyber crime.

2. Age groups, Risky Cyber security Behaviours and Attitudes towards Cyber security

The difference in attitudes towards cyber security according to age groups is an interesting result, with individuals in the higher age bracket demonstrating a more positive attitude towards cyber security. A potential reason for this could be linked to the personality trait of conscientiousness, associated with the propensity to follow rules and norms that are set by society (Jackson et al., 2009). The trait is also linked to planning, delay in gratification, and the ability to control impulses, and has been shown to increase with age (Jackson et al., 2009). It could be that those individuals in the higher age bracket are more conscientious and see engaging in good cyber security practices as being an essential part of their working life. Previous research exploring information security awareness has also noted that conscientiousness significantly explained variance in ISA

(McCormac et al., 2016). In the absence of the actual differences in conscientiousness according to age groups, this suggestion is presented as conjecture, but provides the basis for potential further research in this area.

The frequency with which individuals engaged in risky cyber security behaviours also presented a similar age divide, with those in the younger age group engaging in more frequent risky activities. (McCormac et al., 2017) previously noted a linear relationship between age and information security awareness, with better awareness coming with older age. There are a variety of potential reasons for such a trend, a key one being related to aspects of risk aversion. Previous work has found that younger people are less risk adverse, making them prone to engage in more risk taking behaviours (Reyna & Farley, 2006). However, such a suggestion is problematic in light of the findings from McCormac et al. (2017) who found a significant relationship between age and information security awareness even when risk-taking propensity was controlled for. This suggests that another factor outside of age differences in risk taking influences engagement in information security awareness, potentially also linked to difference in personality traits such as conscientiousness.

3. Company Size, Risky Cyber security Behaviours and Attitudes towards Cyber security

Significant differences for risky cyber security behaviours and attitudes towards cyber security in relation to the size of the company for which the individual was working were also noted. It is interesting to note that those working with companies with 250 or more employees had the highest level of engagement in risky cyber security behaviours. Again, without engaging in further research the reasons for such a difference remain unclear. On the one hand it may be that larger organizations have better communication systems or effective cyber security measures due to larger budgets. Risky behaviours demonstrate a similar pattern, but in this instance there appears to be a level at which risky behaviour plateaus in the 51-250 sized company category, and then drops sharply in organizations over 250. Individuals employed by larger organizations may be made more aware of the risks of engaging in dubious cyber security practices, which again links to potential differences in budget and organizational polices. As this information was not collected in the context of the present study, it would be good to establish this link in further empirical work in this area.

Conclusion

The findings from the present study serve to highlight interplay between cyber security attitudes and behaviours of employees. In terms of risky cyber security behaviours, the majority of employees questioned still engaged in some form of activity that in turn increased the likelihood of a breach in cyber security. Behaviours such as the use of the same password for multiple websites, sharing passwords with colleagues, and clicking on links in emails are all active parts of most information security policies, but are still evident in this sample. Aspects such as lack of skills, knowledge and awareness were seen as the key barriers for individuals engaging in active cyber security, presenting a pathway for further research in this area.

The research and the tools presented within this study are intended to be used further in a practical manner and should be viewed as being reactive, not only in terms of the development of new technologies but also additional policies in the context of cyber

security. The study found evidence that businesses and/or the public are unsure about how to report a cyber crime event, so an increase in education and awareness of the process would enhance the ease of reporting. Although Action Fraud and the National Fraud Intelligence Bureau (NFIB) were not mentioned specifically in the survey, the results highlighted an apparent lack of knowledge as to how the police take reports of cyber crime and how it is dealt with. There might be a case for ensuring that all customer-facing officers and staff can recognize a case of cyber crime when it is reported to them, and that they too, can signpost the customer to the reporting facilities (e.g. Action Fraud) with ease. As 58% of those who completed the survey were unaware of prevention or protection measures against cyber crime, the Fraud Defence Test[3] might prove a valuable place to start.

Limitations to the present research

The research presented here is not without its limitations. The scales presented rely heavily on self-reported data from participants about their activities over a period of one month. It may be that the individual is presenting an ideal representation of their cyber security behaviour rather than their actual behaviours, perhaps in part due to suspicion that their employers might use such information (Hadlington & Parsons, 2017).

The two scales presented here also need further testing with a wider and more varied group of participants. Only through further use of the scales in wider and more varied populations, as well as continued assessment of their validity and reliability activities, can their usability in the context of practical research situations be established. The comparison of the risky cyber security behaviours questionnaire to existing scales such as the SeBIS and correlated personality factors would also be another step in the research process, as well as exploring other potential individual differences (e.g. altruism, work identity, work locus of control).

Acknowledgements

This work was funded as part of the East Midlands Police Academic Collaboration (EMPAC) project under HEFCE fund JO4. This paper is the second half of a dataset, with the first part being previously published in: Hadlington, L. (2017). Human factors in cyber security; examining the link between Internet addiction, impulsivity, attitudes towards cyber security, and risky cyber security behaviours. *Heliyon, 3*(7), e00346. doi: 10.1016/j.heliyon.2017.e00346.

References

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2016). Gender difference and employees' cyber security behaviors. *Computers in Human Behavior*, *69*, 437–443. doi: 10.1016/j.chb.2016.12.040.

Bishop, M., Gollmann, D., Hunker, J., and Probst, C. W. (2008). Countering insider threats. In *Dagstuhl Seminar Proceedings 08302* (pp. 1–18). Retrieved from http://vesta.informatik.rwth-aachen.de/opus/volltexte/2008/1793/pdf/08302.SWM.1793.pdf.

Briney, A., & Prince, F. (2002). Does Size Matter ? The Size of your organisation may be

[3] (Action Fraud website, http://www.actionfraud.police.uk/news/take-the-fraud-defence-test-and-protect-yourself-jan17)

the single biggest barometer of IT security's effectiveness. *ISM Survey*, (September).

Claycomb, W., Huth, C., & Flynn, L. (2012). Chronological examination of insider threat sabotage: preliminary observations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *3*(4), 4–20. Retrieved from http://isyou.info/jowua/papers/jowua-v3n4-1.pdf.

CPNI. (2013). *CPNI Insider Data Collection Study: Report of Main Findings*. London.

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. *Proceeding of the Twenty-Sixth Annual CHI Conference on Human Factors in Computing Systems - CHI '08*, 1065. doi: 10.1145/1357054.1357219.

Egelman, S., and Peer, E. (2015a). Predicting Privacy and Security Attitudes. *Computers and Society: The Newletter of ACM SIGCAS*, *45*(1), 22–28. doi: 10.1145/2738210.2738215.

Egelman, S., & Peer, E. (2015b). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, *1*, 2873–2882. https://doi.org/10.1145/2702123.2702249.

Greitzer, F., Kangas, L., Noonan, C., & Dalton, A. (2010). *Identifying at-risk employees: A behavioral model for predicting potential insider threats*. Retrieved from http://www.pnl.gov/main/publications/external/technical_reports/PNNL-19665.pdf.

Hadlington, L. (2017). Human factors in cyber security; examining the link between Internet addiction, impulsivity, attitudes towards cyber security, and risky cyber security behaviours. *Heliyon*, *3*(7), e00346. doi: 10.1016/j.heliyon.2017.e00346.

Hadlington, L., & Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior, and Social Networking*, *20*(9), cyber.2017.0239. doi: 0.1089/cyber.2017.0239.

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

Herath, T., & Rao, H. (2009b). Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi: 10.1057/ejis.2009.6.

Hunker, J., & Probst, C. (2011). Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1), 4–27. Retrieved from http://isyou.info/jowua/papers/jowua-v2n1-1.pdf.

Jackson, J. ., Walton, K., Harms, P. D., Bogg, T., Wood, D., Lodi-Smith, J., Roberts, B. W. (2009). Not all Conscientiousness Scales Change Alike: A Multimethod, Multisample Study of Age Differences in the Facets of Conscientiousness. *Journal of Personality and Social Psychology*, *96*(52), 446–459. doi: 10.1038/jid.2014.371.

Keeney, M. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors, (May). Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Insider+Threat+Study+:+Computer+System+Sabotage+in+Critical+Infrastructure+Sectors#0.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M.

(2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. doi: 10.1016/j.chb.2016.11.065.

Osborn, E. (2015). *Business vs Technology : Sources of the Perceived Lack of Cyber Security in SMEs*. *Centre for Doctoral Training in Cyber Security*.

Probst, C., Hunker, J., Gollmann, D., and Bishop, M. (2010). *Insider Threats in Cyber Security*. *Vasa*. New York: Springer. Retrieved from http://link.springer.com/content/pdf/10.1007/978-1-4419-7133-3.pdf.

Reyna, V. F., & Farley, F. (2006). Risk and rationality in adolescent decision making: Implications for theory, practice, and public policy. *Psychological Science in the Public Interest, Supplement*, 7(1), 1–44. doi: 10.1111/j.1529-1006.2006.00026.x.

Sasse, M., & Flechais, I. (2005). Usable Security: Why Do We Need It? How Do We Get It? In L. F. Cranor and S. Garfinkel (Eds.), *Security and Usability* (pp. 13–30). Sebastopol, CA: O'Reilly Publishing. Retrieved from http://discovery.ucl.ac.uk/20345.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, 373–382. https://doi.org/10.1145/1753326.1753383.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. *IEEE Symposium on Security and Privacy*, 1–14. https://doi.org/10.1109/SP.2016.26.