Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

Employee Information Security Beliefs in the Home Environment

J. Omidosu and J. Ophoff

Dept. of Information Systems, University of Cape Town, Cape Town, South Africa
e-mail: omdjos001@myuct.ac.za; jacques.ophoff@uct.ac.za

Abstract

As information and communication technology adoption increases it changes the way organizations, government agencies, and individuals view security. Modern technologies have expanded security vulnerability beyond the organizational environment, as employees' access to information is no longer physically constrained and often occurs in the home environment. This study investigates the beliefs influencing employee information security behaviour in the home environment. A qualitative research approach was adopted, with the theory of planned behaviour used as research lens. Thematic analysis of interview data from 19 participants is reported. The research findings present a range of behavioural, normative, and control beliefs influencing employee information security behaviour in the home environment. The research contributes to the behavioural information security domain by expanding the understanding of beliefs influencing employee security behaviour. Using this knowledge management and security experts can develop more effective human-centred interventions to motivate employee adoption of security measures.

Keywords

Information Security Beliefs, Home Environment, Theory of Planned Behaviour

1. Introduction

Organizational infrastructure ranging from banking, e-commerce, telecommunication, government, to education are inter-networked with modern technology. These systems continue to grow at a fast rate due to increased adoption of modern information and communication technologies (ICTs) such as cloud computing, bring your own device, the Internet of things, etc. The proper functioning of a system depends on its security, but these systems have extended organizational vulnerability to emerging cyber threats (Potts, 2012).

Employee work scope is no longer limited to the work environment and an employee can have remote access to organizational information and perform work-related tasks in the home environment. The adoption of modern ICTs allows an employee to have increased remote access to confidential information, thereby exposing the organization to internal and external threats (Warren & Leitch, 2010). Information security is vital when an employee carries out tasks in the organizational context and when accessing information using home computing or mobile devices, which may not be managed by the organization.

A greater percentage of the security breaches experienced by an organization is a result of an employee violating organizational policies (Sommestad et al., 2015). To ensure the security of information assets the organization, ICTs, and human resources play vital roles (Safa et al., 2016). Adequate security measures do not come with deployed computing systems, but requires configuration of applications, supporting software, effective choice of passwords, frequent updates and recent patches, etc. (Adele et al., 2012). Most security measures provide technical solutions, which are inadequate to provide total security solutions (Herath & Rao, 2009). While software and hardware security measures are important, the individual user's behaviour and social factors play an essential role in ensuring information security (Liang & Xue, 2010).

The role of the human factor in ensuring security is important, hence the need for a human-centred approach to ensure a secure environment. This requires a holistic understanding of the security beliefs of computer users' (Shillair & Dutton, 2016; Crossler & Bélanger, 2017). This research aims to expand the understanding of beliefs influencing employee information security behaviour (ISB). Current security research has not fully explored the beliefs that influence the adoption of security measures and, more specifically, limited research has analysed employee beliefs in the home environment. Al-Lozi & Papazafeiropoulou (2012) argued that computer users in a home environment are influenced by social, behavioural, and technical ability. The research question guiding this research is: *What are the beliefs influencing employee ISB in the home environment?*

The paper proceeds with an overview of prior work on ISB as well as the theoretical model which was adopted. Next, the research methodology is discussed, followed by data analysis and a discussion of the research findings. The conclusion summarises the results, discusses research limitation and proposes areas for future work.

2. Literature Review

Several perspectives have been adopted to study ISB ranging from the technical design of security measures, management approaches, organizational approaches to mitigate the threat, motivating compliance, and recently cognitive approaches. A systematic literature review was conducted to evaluate literature relating to ISB and topics that align with the research question.

2.1. Information Security

Information security is defined as "protecting organizational information, hardware and systems used in transmitting and storing confidential information" (Mattord & Whitman, 2012, p. 588). This highlights the importance of information assets, hardware, transmission channels, and storage. The confidentiality, integrity, and availability of information are important regardless of context (Mattord & Whitman, 2012). As organizational dependence on ICTs has increased cyber-attacks which have become a growing concern in the public and private sector. Research in information security has explored measures to prevent intrusions of organizational

systems (Choo, 2011), information systems misuse, computer abuse, and information security compliance (Bulgurcu et al., 2010; D'Arcy et al., 2009; Hu et al., 2012).

An understanding of employees' information security beliefs can enhance adoption of information security technologies and practices. Crossler et al. (2013) identified behavioural information security as a subset of information security which is concerned with the behaviours that involve protecting information and the systems which include the hardware and network structure. Behavioural information security research has focused on awareness training, fear appeals, a culture motivating security, sanctions, and monitoring employees (Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath & Rao, 2009; Hu et al., 2012). When security measures are effectively adopted it reduces security risks (Harrison & White, 2010).

An employee who carries out an organizational task from home can be a source of vulnerability through which an organization is exploited. Employees should be motivated to take personal responsibility and make a self-conscious effort towards the safety of their information and computing devices. Bulgurcu et al. (2010) defined employee attitude towards a behaviour as a measure of an employee's belief in the consequence that adoption will produce the desired result. Employees' belief towards information security will influence their attitude towards security measures.

Social norms also influence employee ISB. The opinion of people close to the employee plays a key role in influencing the intention to practice information security (Ifinedo, 2012; Johnston & Warkentin, 2010). Chu et al. (2015) argued that social influence depends on the environment, influencing factors, and beliefs. A major influencing factor is the organization's security management approach (Bulgurcu et al., 2010).

Perceived behavioural control is argued to be a good predictor of behaviour (Chu et al., 2015). An employee can be concerned about a problem, but that is different from having the control to perform an action (Anderson & Agarwal, 2010). An employee must believe in her ability to provide needed security measures and take responsibility for active control to perform needed measures. Common theories adopted to study ISB include the theory of planned behaviour (TPB) and Protection Motivation Theory (Adele et al., 2012). This study adopts TPB as the lens for the research.

2.2. Theory of Planned Behaviour

Ajzen (1991) developed TPB which has been widely accepted and used by scholars in information systems. In the context of this research, the ISB of a computer user in the home environment is influenced by social norms, behavioural control, and technical ability (Al-Lozi & Papazafeiropoulou, 2012) making TPB an ideal model to analyse the security behaviour beliefs of an employee.

TPB argues that behavioural, normative, and control beliefs form attitude, subjective norms, and perceived behavioural control respectively. These beliefs and factors

define an individual's intention and subsequently determines behaviour (Ajzen, 1991). To understand the contextual beliefs of the research interest, approaches such as in-depth interviews, focus groups, or open-ended questions can be used to gain a deeper understanding of beliefs influencing an individual's behaviour (Francis et al., 2004).

3. Research Methodology

To gain deeper insight into beliefs influencing employee ISB, the research adopts a qualitative research approach. The research assumed an interpretive view, which argues for multiple realities about the beliefs influencing individuals. The ontological assumptions were subjective, which allowed a shared understanding with participants (Saunders et al., 2015). A deductive approach to theory was adopted as it aims "to test the concept and pattern from a known theory" (Bhattacherjee, 2012, p. 3). TPB was adopted to aid mapping of research findings.

The unit of analysis was at an individual level. Francis et al. (2004, p. 25) recommended that "the sample be selected from the population of interest where there is variation in the performance of the behaviour to be investigated." Employees from a university in South Africa who access organizational information from the home environment were the sample frame. The sample frame is argued as suitable because employees remotely use several online systems, which are vulnerable to cyber-attacks, phishing, denial of service, and spyware (Watts et al., 2017). With the vast amount of resources at universities and the need to ensure the privacy of the data, universities are increasingly becoming targets for cyber-attacks.

Participants from different faculties were interviewed as variation regarding security beliefs may occur. A random probability sampling technique was used. A bulk email was sent to university employees (administrative and academic) with those interested in being interviewed responding to the email. An interview guide was designed based on the recommended TPB approach in literature and refined to meet the research objective (Ajzen, 2002; Francis, et al., 2010). A semi-structured interview in the form of face-to-face narrative inquiry with participants was adopted to collect data.

To ensure rigor and generalizability of research findings recommendations by Bhattacherjee (2012) and Saunders et al. (2015) were followed. Data collection stopped at saturation, defined as "the point of data collection when no new additional data are found that develop aspects of a conceptual category" (Francis et al., 2010, p. 1230). After 10 interviews data analysis was performed and served as the initial analysis point to identify emerging themes. After 17 interviews data saturation was reached, as no new themes emerged. However, two more interviews were conducted to ensure that saturation was reached. The sample size is comparable to two similar studies reported in Francis et al. (2010) with saturation after 14 and 17 interviews respectively.

4. Analysis and Findings

A theory-based thematic analysis was chosen for data analysis. Thematic analysis is a method for "identifying patterns of meaning in a dataset" (Joffe, 2012, p. 209). This allowed the identification of emerging themes from the interviews. NVivo, a computer-assisted qualitative data analysis software (CAQDAS) was used for analysis.

In total there were 19 participants. The gender profile was 58% male and 42% female. Participant age ranges included: 16% between 19-30 years, 53% between 31-40 years, 5% between 41-50 years, and 26% between 51-60 years. In a self-evaluation of IT literacy on a 5-point scale 53% of participants rated themselves as very competent (5), 37% competent (4), and 11% average (3). The demographic data indicate a range of profiles with good IT literacy.

4.1. Behavioural Beliefs

The behavioural beliefs examined the benefits and drawbacks of adopting security measures. The greater a threat is and believed important, the greater the chance that the employee will have a positive attitude towards ISB (Liang & Xue, 2010). A positive attitude will lead to a greater intention to adopt security measures. Prior research also shows that employees who believe in the response efficacy will adopt security measures (e.g. Bulgurcu et al., 2010).

The research findings reveal that employee adoption of security measures in the home environment is influenced by a belief that security measures ought to provide favourable utilization outcomes. Such outcomes include preventing severe attacks, financial loss, or loss of data. Participant 2 stated: *"Adopting information security technologies and practices helps in protecting my personal information, protects my financial information and maintenance of the laptop and devices that I use at home, as it will last longer."*

There is also a desire for privacy, aiming to prevent unauthorized access to confidential information. Participant 1 stated: *"The most important thing as I said is privacy, I care so much about my privacy. Everything that I own is locked-locked-locked before you can get to anything. For example, my phone now, there is a lot of pictures of me and my kids, emails and calls that I received. It's like my whole life is in here. So, I really have to make sure I protect it."*

The perceived level of vulnerability is a measure of the likelihood that the employee's device is vulnerable to attack. When a threat is perceived, a behaviour is adopted correlating to the level of vulnerability (Ifinedo, 2012). Participant 8 stated: *"I am very scared of losing my data and because of that the security measure that I have taken is to use iCloud. So, in case anything happens to my devices I can protect them or wipe them remotely."* If the response efficacy of adopted security measures is not certain the motivation to adopt needed security measures may be hindered.

4.2. Normative Beliefs

Normative beliefs measured individuals or groups of people who enhance or pose a challenge to the adoption of security measures in the home environment. The normative beliefs include the influence of social environments on employees' security behaviour, such as the organizational influence in terms of policy, culture, the behaviour of other employees in an organization. Participant 15 stated: *"I have learnt a lot here with security at the University so I tend to follow the same regime on my home computer, especially when I use my own computer to work and to link to my organisation desktop."*

Information via the media (news) also plays an important role as Participant 4 stated: *"From the media, you hear news of credit card details of people stolen or people losing files. So, the environment, the media when you hear the negative effects even though it has not happened to me. It's on the news, I kind of become more security conscious as I don't want this to happen to me."* IT blogs, magazines, friends, family, colleagues, and financial institutions are all social factors influencing the security beliefs of employees. The influence of financial institutions (e.g. banks) is a result of the frequent security awareness information which they distribute and leveraging security technologies via online banking and mobile platforms. Other researchers also found social influence to be an important element that influences computer users ISB (e.g. Herath & Rao, 2009; Johnston & Warkentin, 2010).

It was also found that IT professionals, regulatory bodies, and people with knowledge influence employee ISB in the home environment. Participant 14 stated: *"What I have implemented, the various bits and pieces, I am obviously motivated by the SANS Institute as they do communicate certain standards on information security principles."* The role of knowledgeable peers was illustrated by Participant 11 who stated: *"I look at my colleagues and listen to them and it is fascinating, they are able to help me understand why it is so important to be cyber secure, so I look up to them."*

The connotation associated with hackers, and the risk of them using vulnerabilities for financial gain, seems to influence employee ISB. Participant 16 stated: *"The people that would influence me to adopt the security measure would be those who have a negative connotation to them, people like hackers, and people who try and get into your information. They would influence anybody to want to adopt higher security measures as you do not want these people accessing your information."*

It was also found that prior experiences of security issues by the employee, or people close to the employee, influences ISB. This is in line with previous research on prior security experiences (e.g. Ng et al., 2009; Anwar, et al., 2017). Lastly, the reputation of software and operating systems influence employee ISB in the home environment. Participant 8 stated: *"I use macOS because it is much more secure than other operating systems. I don't really worry that much about viruses as I know that virus doesn't really affect macOS when I am using flashes, there are no worries."*

4.3. Control Beliefs

The control beliefs measured factors that enhance or hinder adoption of information security measures in a home environment (Ajzen, 1991). If security measures are not usable and require more effort the employee is often demotivated to adopt such measures. Participant 1 argued that *"the biggest challenge with security measures, you have to remember a lot of things, a lot of passwords, for the website, you need to remember the password to get to your computer, after which there is another password to do something else."* The need for facilitating conditions in terms of knowledge needed to implement required technologies and practices is also important. Participant 19 stated: *"I will say I still lack certain IT knowledge because if I download software for work on a device that I take home if there is a conflict in downloading the software I lack the knowledge on what to do."*

Cost in terms of money, bandwidth, and time (e.g. seeking and reading awareness information/newsletters, running updates) are believed to pose a challenge to employee's ISB in the home environment. Participant 12 argued that *"it has to do with a connection that you are using, you have to pay for it and some of the programs or some of the processes you have to activate and there is a cost element attached to it."* Lack of technical skills (e.g. if employees do not possess the skills to install required security technologies and run updates) it makes it difficult to adopt ISBs. Participant 4 stated: *"Technical know-how, sometimes even though I am in the IT field, my area of expertise is not in security, so some of these technologies require an advanced level of experience in security to adopt them."*

When the employee's security beliefs (behavioural, normative, and control) are positive it will result in adopting positive ISBs when accessing organizational information in the home environment. On the other hand, when the beliefs are negative the employee's adoption of ISBs becomes an issue, resulting in the employee being vulnerable to cyber-attacks and the compromise of organizational information.

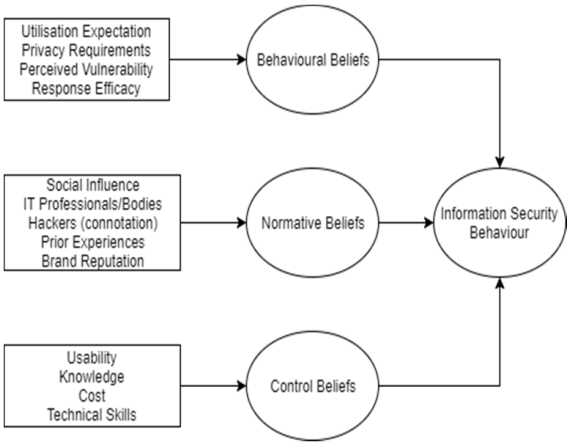

Figure 1: Beliefs influencing employee ISB in the home environment

The research findings are visually summarised in Figure 1. The findings show how employee ISB in the home environment is influenced by behavioural beliefs, normative beliefs, and control beliefs. The findings are in accordance with TPB and if employee beliefs are known they can be motivated to adopt positive ISBs.

5. Conclusion

This research provides insight into employee ISB in the home environment. Theoretically, it validates TPB in the information security domain, applying it to gain a deeper understanding of beliefs influencing employee ISB. The research focused on the beliefs aspect of the TPB and adopted a qualitative approach (which limited prior research has done). Practically, the increasing frequency of cyber-attacks makes this research important and the findings provide insight for managers and security experts to create human-centred interventions to motivate ISB and compliance with security policies.

There is a need for continuous awareness of security measures and practices. Awareness information should be precise, but not too technical. Innovative ways to present information relating to security should be developed. There is brand perception associated with certain companies and IT, however, adoption of security measures is important regardless of brand. Therefore, a more detailed understanding from a human-centred perspective provides rich insight into the beliefs and thought processes driving ISB.

While it was attempted to ensure rigor in the research process some limitations do exist. This includes a limited sample size restricted to participants from the educational sector, which may have influenced their security beliefs. A broader study with a heterogeneous sample is recommended for future research. In addition, future research can build on the identified salient beliefs by evaluating them using a quantitative methodology. Lastly, an investigation into information security best practice could be conducted, for example, at what point can computer users say they are secure?

6. References

Adele, E. H., Indrajit, R., Mark, R. M., & Zinta , B. (2012). The Psychology of Security for the Home Computer User. *2012 IEEE Symposium on Security and Privacy*, (pp. 209-223).

Ajzen, I. (1991). Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Ajzen, I. (2002). Constructing a TPB Questionnaire: Conceptual and Methodological Considerations. Retrieved October 19, 2017 from: https://people.umass.edu/aizen/pdf/tpb.measurement.pdf

Al-Lozi, E., & Papazafeiropoulou, A. (2012). Intention-Based Models: The Theory of Planned Behavior Within the Context of IS. In: Dwivedi Y., Wade M., Schneberger S. (eds) *Information Systems Theory. Integrated Series in Information Systems, (29),* 219-239.

Anderson, C., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cyber security behaviors. *Computers in Human Behavior, 69*, 437-443.

Bhattacherjee, A. (2012). *Social science research: principles, methods, and practices.* Florida: USF Tampa Bay Open Access Textbooks Collection Book 3.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An empirical study of rationality based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Choo, R. (2011). The cyber threat landscape: Challenges and future research directions. *Computer & Security*, 30(8), 719-731.

Chu, A., Chau, P., & So, M. (2015). Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics,* 13(1), 209–225.

Crossler, R. E., Johnson, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information security research. *Computers & Security*, 32, 90-101.

Crossler, R. E., & Bélanger, F. (2017). The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors. *In Proceedings of the 50th Hawaii International Conference on System Sciences.*

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse a deterrence approach. *Information Systems Research, 20*(1), 79–98.

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample? Operationalising data saturation for theory-based interview studies. *Psychology and Health, 25*(10), 1229-1245.

Francis, J., Eccles, M., Johnston, M., Walker, A., Grimshaw, J., Foy, R., & Bonetti, D. (2004). Constructing questionnaires based on the theory of planned behavior. *A manual for health services researchers*, 2-12.

Harrison, K., & White, G. (2010). An empirical study on the effectiveness of common security measures. *In Proceedings 43rd Hawaii International Conference on System Sciences (HICSS)* (pp. 1-7). IEEE.

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hu, Q., Dinec, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organization culture. *Decision Sciences, 43*(4), 615-658.

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

Joffe, H. (2012). *Thematic analysis. Qualitative research methods in mental health and psychotherapy: A guide for students and practitioners* (Vol. 1). Wiley-Blacwell.

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34*(3), 549-566.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Mattord, H., & Whitman, M. (2012). *Principles of information security.* Cengage Learning.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behaviour: A health belief perspective. *Decision Support Systems*, 46 (4), 815-825.

Potts, M. (2012). The state of information security. *Network Security, 2012*(7), 9-11.

Safa, N., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organization. *Computer Fraud & Security,* (2), 15-18.

Saunders, M., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students, (7th Ed.).* Pearson Education India.

Shillair, R., & Dutton, W. H. (2016). Supporting a Cybersecurity Mindset: Getting Internet Users into the Cat and Mouse Game. *Annual Meeting of the Telecommunications Policy Research Conference* (pp. 1-40). Arlington: George Mason University School of Law.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23*(2), 200-217.

Warren, M., & Leitch, S. (2010). Hacker taggers: a new type of hackers. *Information System Frontiers*, 12(4), 425-431.

Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). Cyberbullying in higher education: A literature Review. *Computers in Human Behavior, 69*, 268-274.