Investigating the knowledge-behaviour gap in mitigating personal information compromise

Jasmine Scott
Jacques Ophoff

This is the published version of the conference paper published in the Proceedings of the 12th International Symposium on Human Aspects of Information Security & Assurance, (HAISA 2018)

Scott, J. & Ophoff, J. (2018) 'Investigating the knowledge-behaviour gap in mitigating personal information compromise'. In N. Clarke & S. Furnell (eds.), Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018). Univerisity of Plymouth, Plymouth, pp. 236-245, 12th International Symposium on Human Aspects of Information Security & Assurance, Dundee, UK, 29-31 August 2018.
URL: https://www.cscan.org/?page=openaccess&eid=20&id=393

Investigating the Knowledge-Behaviour Gap in Mitigating Personal Information Compromise

J. Scott and J. Ophoff

Dept. of Information Systems, University of Cape Town, Cape Town, South Africa
e-mail: SCTJAS002@myuct.ac.za; jacques.ophoff@uct.ac.za

Abstract

In response to information threats users instinctively increase security measures, such as firewalls and anti-virus software. However, users do not give enough attention to their behaviour, more specifically, their security behavioural practices. This paper proposes that the knowledge-behaviour gap affects a user's security behavioural practices and this, in effect, threatens personal information security. The knowledge-behaviour gap assesses why users do not put their information security and privacy knowledge into practice. The Information-Motivation-Behavioural Skills Model is used to highlight the different factors which affect the knowledge-behaviour gap, with empirical data collected using an online survey. Despite the wide conformity of opinions within literature, a key finding of this research is that users' awareness of information security threats has an insignificant effect on their self-reported preventive behaviour. The significance of this finding is that users require a deeper technical understanding of information security threats to engage in effective preventive behaviour.

Keywords

Information Security; Personal Information Compromise; Behavioural Skills; Motivation; Preventive Behaviour; Knowledge-Behaviour Gap; Information-Motivation-Behavioural (IMB) Skills Model

1 Introduction

There are numerous online threats to users' personal information. In recent years, privacy breaches have also risen at an unprecedented rate; each year approximately 700 privacy breaches are publicly reported in the United States (Fortier & Burkell, 2015). In response to these attacks users instinctively add security measures, but the effectiveness of these measures depends on self-efficacy to ensure that they are not bypassed. The ability to configure and use security measures correctly is often overlooked but is a vital factor in mitigating personal information risks.

It has been shown that knowledge is a predictor of security behaviour (Parsons et al., 2014). The wider the gap between users' information security and privacy knowledge, and their behaviour, the more likely they are to fall victim to personal information attacks, such as identity theft (Crossler & Belanger, 2017). Crossler and Belanger also suggest that a knowledge-belief gap affects how users engage in security and privacy behaviours, thus affecting the broader knowledge-behaviour gap. The primary research question to be addressed in this study is: *How does the knowledge-behaviour gap affect user behaviour associated with the mitigation of personal information*

compromise? This study uses the Information-Motivation-Behavioural (IMB) Skills Model as a theoretical framework to examine the knowledge-belief gap.

The remainder of this paper is structured as follows. First a review of relevant literature leads to the development of our research hypotheses. Next the research methodology is briefly explained. Data analysis and a discussion of the results follow. Lastly a summary and ideas for future work are given.

2 Background

Users have distinct levels of knowledge of security and privacy threats. In addition, "what an individual thinks he can do may be different from what the individual's actual knowledge is" (Crossler & Belanger, 2017, p. 4075). This describes the essence of the knowledge-belief gap. To protect oneself against personal information threats, users should want to protect themselves as well as have the necessary skills to do so.

If users do not have the knowledge to protect their personal information, they put themselves at a greater risk of identity and information theft. Moreover, even if users believe to have high competency in the use of technology, they still need actual knowledge to take the necessary steps to engage in a preventive behaviour. Therefore, the greater the disparity between users' actual and perceived knowledge, the more likely they are to put their personal information at risk. This is because their actual skills do not align with what they require to protect their information (Crossler & Belanger, 2017). Simply listing what to do and what not to do regarding security and privacy behaviour has a limited impact on security measures; both perceived and actual behaviour must be considered to implement effective security measures (Rhee et al., 2009).

2.1 Knowledge and Beliefs

When one assesses the 'knowledge' aspect of the knowledge-belief gap, a user's information/awareness of potential security threats and their consequences are considered. This is defined as, "both behaviour-related information and 'myths/heuristics that permit automatic or cognitively effortless behaviour-related decision-making" (Chang et al., 2014, p. 173). Considering the IMB model's link between information and motivation it can be argued that if users possess more information about security threats they should be more motivated to engage in preventive behaviour. This is because the user will be more aware of the severity of information attacks (Crossler & Belanger, 2017). When one assesses the 'belief' aspect of the knowledge-belief gap, a user's perceived confidence at performing a behaviour (self-efficacy), is assessed. Perceived behavioural skills, along with actual skills, are necessary to enact a preventive behaviour (Crossler & Belanger, 2017).

Security of devices such as mobiles and personal computers have become essential as users use these assets in their daily operations. As people are sharing more information on these mobile devices, threats to personal information are multiplying. Often, this is due to users not understanding the consequences of sharing this information (Steijn &

Vedder, 2015). Users might be aware that securing their mobile devices is important, but in many cases, they do not know how to implement this security effectively leaving their devices vulnerable to threats (Miller, 2017).

Privacy breaches can be understood as disclosure of information without consent, and this disclosure can be both intentional and unintentional. Privacy issues have become a major consequence of the 'information age', as users are faced with a trade-off between better service delivery, and the privacy that they need to sacrifice to obtain the improvement in service (Norberg et al., 2007). This sacrifice relates greatly to the users' level of information/awareness in relation to information privacy (Macada & Luciano, 2010).

2.2 Motivation

As security and privacy measures often involve costs (e.g. decreased usability) it may be necessary to motivate users to perform desired actions. These approaches will be specific to users and their personal objectives. Motivation can be organized into two paradigms; intrinsic and extrinsic (Yoo et al., 2012). Intrinsic motivation refers to behaviour which cannot be linked to external outcomes, suggesting that engagement in certain activities is done to provide satisfaction or fulfilment and that the user is inherently interested in the task. Extrinsic motivation is driven by external rewards or performing the activity to avoid negative consequences. Many users are extrinsically motivated to engage in security practices, as they try to avoid personal information threats (Yoo et al., 2012). In these cases, the negative consequences of attacks on personal information motivate users to exercise a preventive behaviour (Wall & Lowry, 2013).

2.3 Self-Efficacy and Behavioural Skills

Self-efficacy is a performance-based measure of perceived capability and is defined as "people's judgments of their capabilities to organize and execute courses of action required to attain designated performances" (Choi et al., 2013, p. 10). Self-efficacy has been a major focal point in evaluating perceived skills and relates to the beliefs that users have about those skills. Research that has been conducted on security and privacy has found that self-efficacy plays a leading role in the regulation and motivation of preventive behaviour, as users' perception of their technical skills affects their level of engagement with technology (Crossler & Belanger, 2017). It leads to positive emotions and cognitions as users feel more confident with their ability to protect their information (Schunk, 1995). This confidence creates the motivation to comply with security policies, as users believe that they have a better understanding of the security risks that they face (Wall & Lowry, 2013).

Users have perceptions of their security and privacy skills that have been impacted by past experiences and assessments. Self-efficacy beliefs determine how much time users will devote to setbacks, or how long they will persevere to overcome these setbacks (Bandura et al., 2003). The greater users' perception of their skills and knowledge, the more likely they are to engage in a preventive behaviour and thus

reduce the knowledge-behaviour gap. This is because the user becomes more aware of the negative consequences associated with potential security threats.

2.4 Information-Motivation-Behavioural Skills Model

The IMB model has been a significant tool in explaining health-related behaviour but has not been widely used to investigate security preventive behaviour (Crossler & Belanger, 2017). Its usage is applicable in the information security and privacy area, as it is also being used to investigate the nature of users' choices to engage in a behaviour. As shown in Figure 1, the model's constructs include *information*, *motivation*, and *behavioural skills*, which are required to engage in *preventive behaviour* (Chang et al., 2014). Using the model, we theorise that preventive behaviour encompasses users' information/awareness of information security threats, their motivation to engage in a security practice, and both the actual and perceived behavioural skills that they possess. To the extent that users are well informed, motivated to act, and possess the requisite behavioural skills, it is probable that they will experience positive security outcomes (Fisher et al., 2003).

According to the IMB model, information is a prerequisite for enacting certain behaviour. This includes information about security threats, behaviour-related information about effective preventive measures, and policies or informal rules to aid in decision-making. In the case of information security and privacy, this would be all the preventive information regarding how to protect oneself online, the types of security threats, and the effects of these threats. Users who are mindful of information security and privacy have a more positive view on engaging in security mechanisms, and this attitude generally leads to compliance intentions (Crossler & Belanger, 2017).

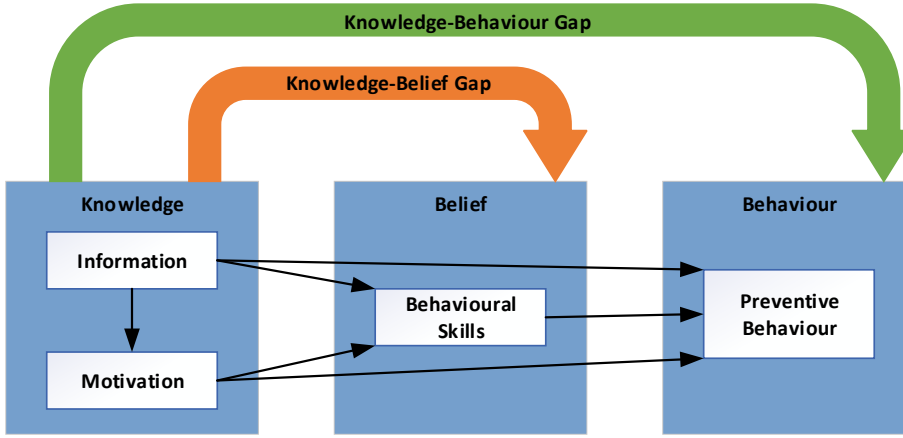

Figure 1: IMB Model Constructs and Knowledge Gaps

Motivation refers to how driven users are to adopt information security and privacy behaviour, and how likely it is for them to continue this behaviour for a prolonged period. Finally, users require specific behavioural skills to increase the likelihood of

them engaging in security and privacy behaviour. From this the following hypotheses are derived:

H1: Information (knowledge) about security and privacy threats will have a positive effect on self-reported preventive behaviour.

H2: Motivation to perform security- and privacy-related practices will have a positive effect on self-reported preventive behaviour.

H3: Behavioural skills (self-efficacy) will have a positive effect on self-reported preventive behaviour.

H4: Information about security and privacy threats will have a positive effect on motivation.

H5: Information about security and privacy threats will have a positive effect on behavioural skills.

H6: Motivation to perform security- and privacy-related practices will have a positive effect on behavioural skills.

3 Methodology

The study adopted a positivist research philosophy, using a quantitative method to collect data. A survey strategy using a questionnaire was used to collect data about participants in a systematic manner. Questions for each of the IMB constructs were adopted from previous studies: behavioural skills (self-efficacy) from Rhee et al. (2009); motivation from Belanger et al. (2017); information (knowledge) from Bulgurcu et al. (2010); and preventive behaviour from Dupuis et al. (2016). All questions used a 7-point Likert scale (strongly disagree to strongly agree).

The survey was created and managed in Qualtrics (http://qualtrics.com/) and distributed through Prolific (https://prolific.ac/) which is an online platform connecting researchers and participants. Simple random (probability) sampling was used. Participants were paid to complete the questionnaire, according to the prescribed platform rates.

To ensure the resulting dataset was free of errors a data-cleaning process was performed in which incomplete and unengaged responses were removed. Analysis of the cleaned data was done using Partial Least Square Structural Equation Modelling (PLS-SEM). PLS-SEM is "an ordinary least squares (OLS) regression-based method which uses available data to estimate the path relationships in the model" (Hair et al., 2013, p. 14). The approach is suitable for validating predictive models. The SmartPLS 3 (https://www.smartpls.com/) software was used for analysis.

4 Data Analysis and Discussion

A total of 267 questionnaire responses were received. 18 responses were removed during the data-cleaning process. The final dataset consisted of 249 valid responses which was split 42% (n=105) male, 57% (n=143) female, and one preferring not to answer. The age distribution was positively skewed with most respondents being between the ages of 26 and 35 years old (n=102), followed by respondents between the ages of 36-45 years old (n=51). A single question regarding the respondent's knowledge of computers and IT was asked using a 7-point scale, with 34% self-reporting that their IT knowledge was Above Average, followed by Average (24%), and Good (19%). Only two respondents had a self-perception that their IT knowledge was Poor. The reported mean was 4.76, indicating that generally respondents perceived their IT knowledge to be average. The assumption is therefore that respondents have a basic understanding of information security threats.

4.1 Analysis of the Measurement Model

The IMB model used in this study consists of both reflective and formative constructs. Information, Motivation, and Behavioural Skills are reflective constructs, whereas Self-Reported Preventive Behaviour is a formative construct. "Reflective measurement models are assessed on their internal consistency reliability and validity. The criteria for reflective measurement models cannot be universally applied to formative measurement models" (Hair et al., 2014, p. 98). Therefore, different evaluation techniques were used to assess the results of these constructs.

As recommended, reflective indicators which had an outer loading of less than 0.40 were removed (Hair et al., 2014). Regarding internal consistency reliability all constructs were above the recommended composite reliability threshold (0.70). Regarding convergent validity the average variance extracted (AVE) for variables were above the recommended threshold (0.50). Finally, discriminant validity was measured using the heterotrait-monotrait (HTMT) ratio of correlations, which showed that all variables were below the 0.90 threshold. All model evaluation criteria were met, providing support for the measures' reliability and validity.

Formative measurement constructs were assessed using three steps: establishing construct validity through factor analysis, examining any collinearity issues, and significance of path coefficients. In this process two measurement items were removed, after which tests showed satisfactory results.

4.2 Analysis of the Structural Model

The structural model was tested to estimate the path coefficients, which calculates the strength of the relationships between variables. The coefficients of determination (R^2) values were estimated to determine the variance explained by the independent variables. The analysis shows that 55.9% of the variation in Behavioural Skills can be explained by the variation in Information and Motivation. Similarly, 21.1% of the variation in Motivation can be explained by the variation in Information. Finally,

64.7% of the variation in Self-Reported Preventive Behaviour can be explained by the variation in Information, Motivation, and Behavioural Skills. Compared to previous studies in information security with similar variables, the values show a medium to high effect size.

Bootstrapping with 5,000 samples (recommended by Hair et al., 2014) was used to test the significance of the structural paths (hypotheses). The bootstrapping results show that, except for H1, all hypotheses are supported. The PLS path modelling estimation, including path coefficients and p-values, is shown in Figure 2. The results of hypothesis testing are summarised in Table 1.

4.3 Discussion

4.3.1 Information

Despite the conformity of opinions within literature that a user's knowledge about information security threats improves their preventive behaviour, findings show that information has an insignificant effect on self-reported preventive behaviour (H1). The composite reliability values indicate that the construct has high internal consistency, so one can assume that the indicators effectively measured users' knowledge. Our findings contradict the assumption that if a user possesses more information regarding threats, the more likely they are to take preventive measures.

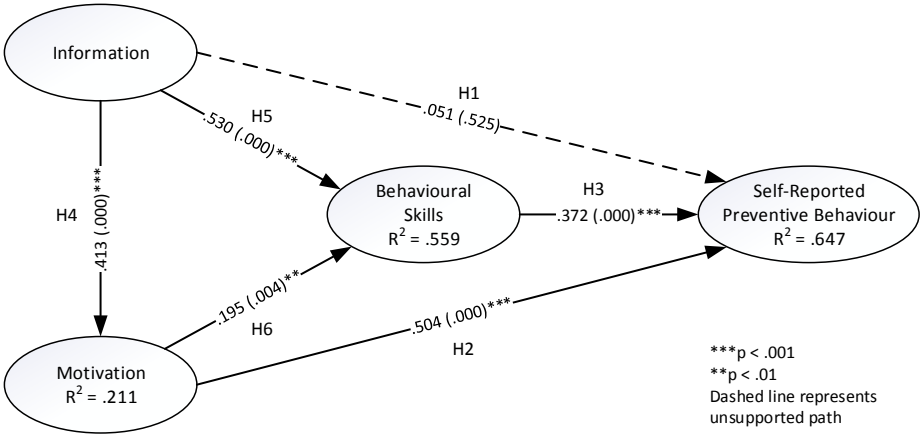

Figure 2: Structural Model Analysis

Hypothesis	Path Coefficient	T Value	P Value	Supported?
H1	.051	.914	p = .525	Not supported
H2	.504	5.000	p < .001	Supported
H3	.372	3.043	p < .001	Supported
H4	.413	6.263	p < .001	Supported
H5	.530	8.661	p < .001	Supported
H6	.195	2.905	p < .01	Supported

Table 1: Overview of Findings

Macada and Luciano (2010) reported that the sacrifices users make regarding their personal information could be related to a lack of general knowledge about IT. Thus, even if users are aware of threats, they require a deeper technical understanding of how to protect their information to prevent personal information compromise.

The relationship between information and behavioural skills (H5) was highly significant. These results are supported by Stajkovic and Luthans (1998), as it was reported that if a user's knowledge of security threats is above average they have a stronger form of self-conviction about their ability to safeguard their resources and personal information.

The relationship between information and motivation (H4) generated a statistically significant result and can be reinforced by Crossler and Belanger (2017) in that the more information users possesses about security threats, the more motivated they will be to engage in a preventive behaviour. This is because the user will have a greater awareness of the consequences of potential security threats.

4.3.2 Motivation

This research sought to test whether motivation drives users to exercise a preventive behaviour; the negative consequences of personal information attacks initiate preventive behaviour. The questionnaire attempted to determine if the key reason for exercising a preventive behaviour was to avoid negative consequence such as viruses. Motivation showed a significant relationship with the self-reported preventive behaviour construct (H2), showing in this survey that users tend to engage in a preventive behaviour to avoid negative consequences such as viruses.

For H6 it had to be determined how motivation and behavioural skills (self-efficacy) were related. It has been reported in literature that self-efficacy is a predictor of security and privacy-related intention (e.g. Bulgurcu et al., 2010). This hypothesis proved to be significant and provide further evidence for this. Schunk (1995) reported that if people perceive that they are performing tasks more successfully, or if they are becoming more competent whilst performing tasks, their motivation increases.

4.3.3 Behavioural Skills

To engage in a preventive behaviour a user must possess specific behavioural skills. These skills include both actual and perceived skills (Crossler & Belanger, 2017). The significant result for H3 reiterates that behavioural skills plays a leading role in the regulation and motivation of users' security behaviour, as perception of technical skills affects their level of engagement with technology.

5 Conclusion

Threats to personal information will always be present if users are engaging with IT. Our research question addressed the proposed gap between knowledge and behaviour, investigating how this affects self-reported preventive behaviour aimed against

personal information compromise. We proposed a theoretical perspective based on the IMB model. Although information was shown to have an insignificant effect on preventive behaviour (H1 was not supported), if users mobilise the motivation and behavioural skills required to effectively engage in a preventive behaviour, they are likely to diminish the knowledge-behaviour gap (H2-H6 was supported). Our results show that the IMB model can be used to investigate information security factors which contribute to these gaps, and how these factors link to a users' preventive behaviour.

Since the research was purely quantitative future research could contribute more depth of understanding through a qualitative methodology, asking what specific preventive behaviour measures users feel they need to improve. A qualitative approach would also work well for the information and motivation constructs to determine specific factors which drive users to engage in a preventive behaviour and their exact level of knowledge of security and privacy threats.

6 Acknowledgement

This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838).

7 References

Bandura, A., Caprara, G. V., Barbaranelli, C., Gerbino, M., & Pastorelli, C. (2003). Role of Affective Self-Regulatory Efficacy in Diverse Spheres of Psychosocial Functioning. Child Development, 74, 769-782.

Belanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. Information & Management, 54(7), 887–901.

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, 523-548.

Chang, S., Choi, S., Kim, S.-A., & Song, M. (2014). Intervention Strategies Based on Information-Motivation-Behavioral Skills Model for Health Behavior Change: A Systematic Review. Asian Nursing Research, 8, 172-181.

Choi, M., Levy, Y., & Anat, H. (2013). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) (pp. 1-19). New York: WISP 2012 Proceedings.

Crossler, R., & Belanger, F. (2017). The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors. Proceedings of the 50th Hawaii International Conference on System Sciences (pp. 4071-4080). Hawaii: Hawaii International Conference on System Sciences.

Dupuis, M., Crossler, R., & Popovsky, B. E. (2016). Measuring the Human Factor in Information Security and Privacy. (pp. 3676-3685). Hawaii: 49th Hawaii International Conference on System Sciences.

Fisher, W., Fisher, J., & Harman, J. (2003). The Information–Motivation–Behavioral Skills Model: A General Social Psychological Approach to Understanding and Promoting Health Behavior. In W. Fisher, J. Fisher, & J. Harman, Social Psychological Foundations of Health and Illness (pp. 82-102). London: Blackwell Publishing Ltd.

Fortier, A., & Burkell, J. (2015). Hidden Online Surveillance: What Librarians Should Know to Protect Their Own Privacy and That of Their Patrons. Information and Technology Libraries, 34, 59-72.

Hair, J., Ringle, C., & Sarstedt, M. (2013). Editorial-partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. Long Range Planning, 46(1-2), 1-12.

Hair, J., Hult, T., Ringle, C., & Sarstedt, M. (2014). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). California: SAGE Publications.

Macada, A., & Luciano, E. (2010). The influence of human factors on vulnerability to information security breaches. Proceedings of the Sixteenth Americas Conference on Information Systems (pp. 1-9). Lima: Americas Conference on Information Systems.

Miller, K. (2017). What We Talk about When We Talk about "Reasonable Cybersecurity": A Proactive and Adaptive Approach. The Computer & Internet Lawyer, 34, 1-8.

Norberg, P., Horne, D., & Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. The Journal of Consumer Affairs, 41, 100-126.

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, 42, 165–176.

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

Schunk, D. (1995). Self-Efficacy, Motivation, and Performance. Journal of Applied Sport Psychology, 7, 112-137.

Stajkovic, A., & Luthans, F. (1998). Social cognitive theory and self-efficacy: going beyond traditional motivational and behavioral approaches. Organisational Dynamics, 26, 62-74.

Steijn, W., & Vedder, A. (2015). Privacy concerns, dead or misunderstood? The perceptions of privacy amongst the young and old. The International Journal of Government & Democracy in the Information Age, 20, 299-311.

Wall, J., & Lowry, P. (2013). Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. Journal of Information Privacy & Security, 9, 52-79.

Yoo, S., Han, S., & Huang, W. (2012). The roles of intrinsic motivators and extrinsic motivators in promoting e-learning in the workplace: A case from South Korea. Computers in Human Behavior, 28, 942-950.