Naïve and Accidental Behaviours that Compromise Information Security: What the Experts Think

D. Calic[1], M. Pattinson[2], K. Parsons[1], M. Butavicius[1] and A. McCormac[1]

[1]Defence Science and Technology Group, Edinburgh, Australia
[2]Adelaide Business School, The University of Adelaide, Australia
e-mail: {dragana.calic; kathryn.parsons; marcus.butavicius;
agata.mccormac}@dsto.defence.gov.au; malcolm.pattinson @adelaide.edu.au

Abstract

The aim of the present study was twofold. First it aimed to elicit Information Security (InfoSec) experts' perceptions about the most important naïve and accidental behaviours that could compromise the InfoSec of an organisation. The second aim was to use these findings to assess the relevance of behaviours that are currently measured by the Human Aspects of Information Security Questionnaire (HAIS-Q), with the intention to further validate the instrument. We employed a qualitative, focus group data collection approach, which enabled rich discussion with InfoSec experts. Fifteen InfoSec experts were asked: *"What naïve and accidental behaviours could compromise the information security of an organisation?"* They brainstormed, discussed and rated the most important behaviours. According to these experts, the three most important behaviours were *sharing passwords*, *not considering the consequences of Social Media (SM)*, and *oversharing information on SM*. It was also found that, of the eleven most important behaviours, rated by the InfoSec experts, eight were part of the HAIS-Q. Furthermore, discussions emphasised the notion of human naivety, lending support to the focus on naïve and accidental behaviours. Finally, our findings demonstrate that behaviours measured by the HAIS-Q are relevant, providing validation for the HAIS-Q.

Keywords

Information Security (InfoSec), InfoSec Behaviour, Human Aspects of Information Security Questionnaire (HAIS-Q), InfoSec Experts, Cyber Security

1. Introduction

It is increasingly recognised that the human aspects of information security (InfoSec) need to be considered. InfoSec has historically relied on technical solutions to counter various threats and vulnerabilities. However, humans, as users of computers, form an integral part of the overall information technology (IT) system, and are considered to be the weakest link in the overarching IT system (e.g., Furnell & Clarke, 2012; Pattinson & Anderson, 2007; Schneier, 2004). Consequently, there has been a shift in the IT literature and practice to try to understand and consider the human aspects. In this paper, we focus on the human aspects of InfoSec.

The aim of the current study was twofold. The first aim was to elicit InfoSec experts' perspectives about the most important naïve and accidental behaviours that could compromise InfoSec of an organisation. The second aim was to use the behaviours generated by InfoSec experts to evaluate the relevance of behaviours currently measured by the Human Aspects of Information Security Questionnaire (HAIS-Q), to further validate the instrument.

In the following sections, we justify the focus on naïve and accidental behaviours, provide an overview of the HAIS-Q, and a brief review of previous research that has involved InfoSec experts. The remainder of this paper describes the workshop methodology and its findings.

1.1. Naïve and Accidental Behaviours

The Global State of Information Security Surveys consistently report that current employees are the most prevalent source of InfoSec threat (Pricewaterhouse Coopers (PWC), 2014, 2015). Naïve and accidental behaviours are thought to be the most frequent source of InfoSec breaches (Schultz, 2005; Wood & Banks, 1993). Interviews within three Australian public service organisations revealed that managers believed that InfoSec breaches were most likely caused by employee naïve and accidental mistakes rather than malicious intent (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2013).

Naïve and accidental behaviours, also referred to as neutral behaviours or naïve mistakes are associated with human errors when using a computer (Crossler et al., 2013; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Stanton, Stam, Mastrangelo, & Jolton, 2005). Naïve and accidental behaviours do not require technical expertise. Examples include using easy-to-guess passwords; opening unsolicited email attachments; not reporting security incidents; and, accessing dubious websites. A better understanding of the types and prevalence and factors associated with these behaviours, could assist with developing strategies and mechanisms that could be used to improve InfoSec awareness.

1.2. The Human Aspects of Information Security Questionnaire (HAIS-Q)

To assess the extent to which naïve and accidental behaviours could compromise the InfoSec of an organisation, the Human Aspects of Cyber Security (HACS) research team developed the HAIS-Q (Parsons et al., 2014; Parsons et al., 2013; Parsons et al., 2015). The HAIS-Q is a psychometric instrument which examines employee knowledge of InfoSec, attitude towards InfoSec, and self-reported InfoSec behaviour. The instrument centres around the following seven focus areas: *Password management, Email use, Internet use, Social media use, Mobile devices, Information handling,* and *Incident reporting*. Each focus area is further divided into three specific InfoSec behaviours. The key elements of interest for the current paper are these specific InfoSec behaviours measured by the HAIS-Q. Table 1 outlines these behaviours and the focus areas associated with each of the behaviours.

Behaviours	InfoSec Area of Focus
Locking workstations Password sharing Choosing a good password	**Password Management**
Forwarding emails Opening attachments IT department level of responsibility	**Email Use**
Installing unauthorised software Accessing dubious websites Inappropriate use of internet	**Internet Use**
Amount of work time spent on SM Consequences of SM Posting about work on SM	**Social Media (SM) Use***
Reporting suspicious individuals Reporting bad behaviour by colleagues Reporting all security incidents	**Incident Reporting**
Physically securing personal electronic devices Sending sensitive information via mobile networks Checking work email via free network	**Mobile Devices***
Disposing of sensitive documents Inserting DVDs / USB devices Leaving sensitive material unsecured	**Information Handling**

*Previously, Social Networking Site Use and Mobile Computing, respectively.

Table 1: InfoSec behaviours as part of the HAIS-Q (Parsons et al., 2014)

As the domain of InfoSec continues to evolve, InfoSec behaviours of importance also change. As a result, the HAIS-Q needs to be regularly reviewed and updated. In this study, InfoSec experts' provided their perceptions for the purposes of assessing the relevance of InfoSec behaviours currently measured by the HAIS-Q, with the aim to validate the instrument. The next section provides a brief overview of previous research that considered the perceptions of InfoSec experts.

1.3. Previous Research: Information Security Experts

In this paper, the term *InfoSec expert* describes a broad range of IT governance professionals, for example, InfoSec auditors, internal auditors, consultants, regulators and chief information officers. These InfoSec practitioners are employed by a range of industries, including banking and financial sectors, accounting, healthcare, government and the public sector, and manufacturing (ISACA, 2015).

IT governance has developed as a result of increased use of IT and the need to address the associated risks. Vroom and Von Solms (2004) argue that IT auditors focus on IT and the technical infrastructure of the organisation. While the traditional auditing approaches consider the finances, technology, security and infrastructure of an organisation, they neglect the human factor, stating that *"auditing is technical in nature and it tends to ignore the human side of operations…."* (Vroom & Von Solms, 2004, p. 193). Vroom and Von Solms (2004) proposed an alternative approach that considered organisational culture, and the individual, the group and organisational level factors that can affect the security of an organisation.

Previous research has rarely focussed on InfoSec practitioners' views, and especially their views about the human aspects of InfoSec. This may be because the human aspect has not commonly been of concern to InfoSec practitioners. One exception is research by Kraemer and Carayon (2007) who conducted sixteen interviews with network administrators and security specialists. The participants discussed elements which, Kraemer and Carayon (2007, pp. 148-151) argued, contribute to human errors in "computer and information security": the individual, task, workplace environment, technology, and the organisation. Interviews revealed that both types of IT experts identified organisational factors (i.e., structure, communication, security culture, and policy) as the most frequent contributors to human errors. The experts did not view the workplace environment and technology elements as important contributors to human errors.

Research is yet to fully examine and understand InfoSec experts' views relevant to the human aspects of InfoSec. As the importance of the human factor in InfoSec becomes increasingly recognised, effective IT governance will be vital to identify and protect against the associated human factors risks. Since effective IT governance relies on InfoSec experts' knowledge and opinions, it is important to understand InfoSec experts' perceptions.

2. Method

Fifteen certified InfoSec experts (13 males and 2 females) participated in one of two workshops. Seven took part in the first workshop and eight in the second, conducted in late 2014. All participants, except one, were members of the Adelaide chapter of ISACA. Previously known as the Information Systems Audit and Control Association, ISACA is an independent, non-profit, international association, concerned with IT governance (ISACA, 2015). Workshop participants have been ISACA members for at least six years, and five participants have been members for twenty years and over. They had experience in a variety of professional IT-related roles such as InfoSec auditors, IT and InfoSec consultants, risk and security specialists. They covered a range of industries such as banking and financial, state and federal government, private consultancy, and the large international accounting firms (i.e., the Big Four).

Each workshop took approximately an hour and was audio recorded. The workshops comprised the following stages:

- **Brainstorm behaviours.** Participants were asked, "*What naïve and accidental behaviours could compromise the information security of an organisation?*" The moderator emphasised the focus on employee naïve and accidental behaviours. As participants brainstormed behaviours, an assistant recorded the generated behaviours, which were displayed on a projected screen, so they could be viewed by all. This enabled discussion of the generated behaviours.

- **Classify behaviours**. Once the brainstorm reached a saturation point, a list of behaviours, including the ones generated during the brainstorm and the HAIS-Q behaviours (i.e., only the HAIS-Q behaviours not raised by the participants), was created. The combined list of behaviours was sorted alphabetically, printed and provided to all participants. They were asked to identify five to seven behaviours which they consider would pose the greatest risk to an organisation's InfoSec. This was completed individually by each participant.

2.1. Analyses

Participants' ratings from both workshops were normalised to account for differences in the number of behaviours selected by participants (i.e., while some participants selected the maximum number of seven behaviours, others selected five or six). The overall scores were then divided by the total number of participants (i.e., 15). The obtained score was used to order the behaviours based on participants' selections. The results are presented (Table 2) and discussed in the next section.

In addition to participants' ratings, analyses also focus on qualitative discussions. The workshop discussions were audio recorded, transcribed, and NVivo10 was used to conduct thematic analysis (QSR International, 2012). Thematic analysis was used to identify common patterns or themes within the data (Braun & Clarke, 2006). In the next section, outcomes of thematic analysis are reported and discussed in terms of experts' ratings.

3. Findings and Discussion

This section is divided into two parts. The first focusses on experts' rankings of the most important InfoSec behaviours, and whether they were measured by the HAIS-Q. The second part focusses on InfoSec practitioner discussions, and provides insight into why the participants thought the behaviours were important.

3.1. The Most Important Behaviours

Our findings validate the relevance of InfoSec behaviours that are currently part of the HAIS-Q. Table 2 presents the most important naïve and accidental behaviours as ranked by InfoSec experts. Eight of these eleven behaviours (73%) were already included in the HAIS-Q. These behaviours also align with all seven InfoSec areas of focus measured by the HAIS-Q (as indicated in the right column). The three behaviours that were not part of the HAIS-Q, as denoted by the asterisk, included: *Oversharing information on SM; Indiscriminate clicking on links;* and, *Reusing the same passwords in multiple places. Indiscriminate clicking on links* was not associated with a specific InfoSec area of focus because it could be associated with more than one focus area (e.g., Internet Use and Email Use).

	Most Important Behaviours	**InfoSec Area of Focus**
1	Sharing passwords	**Password Management**
2	Not considering consequences of SM	**Social Media (SM) Use**
3	Oversharing information on SM*	**Social Media (SM) Use**
4	Accessing dubious websites	**Internet Use**
5	Using unauthorised external media	**Information Handling**
6	Indiscriminate clicking on links*	
7	Reusing the same passwords in multiple places*	**Password Management**
8	Opening an attachment from an untrusted source	**Email Use**
9	Sending sensitive information via mobile networks	**Mobile Devices**
10	Not physically securing personal electronic devices	**Mobile Devices**
11	Not challenging or reporting security incidents	**Incident Reporting**

Table 2: Most important naïve and accidental InfoSec behaviours, as ranked by InfoSec experts

During the workshops, InfoSec experts brainstormed and discussed the naïve and accidental behaviours. These discussions provided an in-depth insight into experts' rankings of the most important behaviours. As shown in Table 2, two of the three most important behaviours related to SM use, and InfoSec experts' discussions frequently focussed on different aspects of SM use and online sharing. Experts predominantly discussed the risks associated with information sharing online:

> *"...sharing too much information that then can be used to compromise accounts or other things."*
>
> *"LinkedIn's probably one of the worst ones because that's where you talk about the work that you've done and how much of that is sensitive..."*
>
> *"That itself is a risk... that you've got undesired audience."*

This is similar to findings by Parsons et al. (2013) who reported that management within Australian public service organisations acknowledged that their organisations had potential SM vulnerabilities, and stated that this is an area where further education is required. Furthermore, the experts' discussions are in line with a plethora of recent research that has focussed on understanding self-disclosure on SM. This is particularly important because it is believed that, while people understand the privacy and security risks associated with SM, they still continue to self-disclose personal information on SM (Dienlin & Trepte, 2015).

3.2. Experts' Discussions: Focus on Naïve and Accidental Behaviours

Experts' discussions strongly focussed on the notion of human naivety and the lack of understanding of InfoSec risks, and these emerged as the most prominent themes.

The majority of this discussion focussed on people's naivety as a result of insufficient understanding of the risk and a lack of InfoSec knowledge.

> *"People are just naïve because they don't understand."*

> *"It's naïve behaviour, not understanding the risks involved."*

> *"[I]t really depends on whether people within the organisation understand the risk and whatever controls are put in there to mitigate the risk."*

> *"So does that just come down to general complacency that this is not going to affect me? ... when you talk about IT security, people are sometimes saying, well it won't affect me, and I'll just go about my work, and then until such time as a process happens, poor password construct or you're getting attacked and then all of a sudden they're saying, oh okay, what did I do to contribute towards that?"*

Participants discussed the importance of training and education as potential ways to manage or reduce these naïve behaviours and improve people's understanding of associated InfoSec risks. They also emphasised the importance of educating employees over solely focusing on technological controls.

> *"This comes back to them understanding the risk and the impact of what you're doing, so they really understand what to do and what not to do."*

> *"...you can't rely on the technical control in all circumstances."*

> *"...if you can have a very good, educated workforce, they're going to be stronger than the IT controls."*

These views are in line with the recent report by Telstra (2014) which found that employee security education and awareness training needed greater focus. Similarly, the recent Pricewaterhouse Coopers (PWC) (2015, p. 18) report noted that, with the increase in cyber threats, "companies are expanding their technology-centred view to include people and processes."

Participants also discussed a number of potential barriers to improved InfoSec, such as training delivery issues and over-training, employee complacency, and, the vulnerabilities associated with training budgets.

> *"But it also could be policy, fatigue, I mean in my organisation we have 13 mandatory trainings that you have to have, OH&S, fraud, corruption, security, and you add them up and there are just too many things to remember."*

> *"But I think it could still come back that now, this group is educated enough, but the complacency factors still seeps in and that's human beings."*

> *"And then of course resources get tight and the first thing that goes out the window is training."*

Similarly, the InfoSec experts noted that security measures are often perceived to hinder and delay work and task completion, leading employees to ignore security measures.

> *"A lot of it is just people wanting to do the job and naively cutting corners to get that done or do whatever's easiest."*

This is consistent with previous findings by Parsons et al. (2013) who reported that management within Australian public service organisations recognised that there can be tensions between the need to abide by security requirements and the need to complete work tasking. Related to this is the notion of risk compensation or risk homeostasis, which suggests that people are generally willing to accept a certain level of risk to effectively complete their tasking. When their surroundings change, people tend to adjust their behaviour to maintain their accepted level of risk (Pattinson & Anderson, 2004; Wilde, 2001). This can be dangerous, however, as people who feel more protected may engage in more risky behaviours.

4. Limitations and Future Directions

A number of possible limitations need to be noted when considering the results of this research. For example, data collection relied on focus groups, which, being interactive and open, enabled rich discussions and access to diverse perspectives. Nonetheless, focus groups can be associated with groupthink, and the possibility that not all participants' views are equally represented, as some participants may have dominated the discussion (Kidd & Parshall, 2000). Also, participants' InfoSec backgrounds and experiences may have influenced their perspectives in terms of the most important naïve and accidental behaviours.

Consequently, we note that this is only one possible form of validation of the HAIS-Q. Further research could focus on other complementary qualitative approaches, such as semi-structured interviews, and structured interviews using the Repertory Grid Technique (RGT). Pattinson, Butavicius, Parsons, McCormac, and Jerram (2015) have previously used the RGT to better understand computer user InfoSec behaviour. Also, quantitative validation of the HAIS-Q could involve test/re-test evaluations, and evaluations with diverse samples, such as employees from different industries and organisations.

With constant evolvement within the InfoSec domain, it is important to ensure that the HAIS-Q is appropriately updated to focus on the most important behaviours. For example, based on the current results, SM-related behaviours are considered very important. It would be interesting to see if this trend continues to hold as SM becomes even more integral to our everyday interactions. Also, as presented earlier, the InfoSec experts identified three behaviours that were not part of the HAIS-Q. As a result, the HAIS-Q has been further developed and updated to incorporate these behaviours.

5. Conclusions

The present study elicited InfoSec experts' perceptions about the most important naïve and accidental behaviours that could compromise InfoSec of an organisation. The three most important behaviours were *sharing passwords*, *not considering the consequences of SM*, and *oversharing information on SM*. These findings were used to assess the relevance of behaviours currently measured by the HAIS-Q, with the intention to further validate the instrument. It was found that, of the eleven most important behaviours, as rated by InfoSec experts, eight were currently in the HAIS-Q. This result provides confirmation that the behaviours measured by the HAIS-Q are relevant, providing further validation for the HAIS-Q.

Furthermore, the InfoSec experts emphasised the notion of human naivety, lending further support to the focus on naïve and accidental behaviours. Human naivety was associated with insufficient understanding of the risk and a lack of InfoSec knowledge. Therefore, education and training were considered as potential ways to manage this, however, noting potential issues associated with training delivery, over-training, employee complacency, and, training budget vulnerabilities. Finally, InfoSec experts noted that security measures can be perceived to hinder and delay work and task completion, leading employees to ignore security measures. Consequently, as the domain of InfoSec continues to evolve, it will be imperative to keep abreast of the most important naïve and accidental behaviours and factors that may affect them.

6. References

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

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

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285-297.

Furnell, S., & Clarke, C. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31, 983-988.

ISACA. (2015). History of ISACA. Retrieved 9 November, 2015, from http://www.isaca.org/About-ISACA/History/Pages/default.aspx

Kidd, P. S., & Parshall, M. B. (2000). Getting the focus and the group: enhancing analytical rigor in focus group research. Qualitative health research, 10(3), 293-308.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied ergonomics, 38(2), 143-154.

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.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013, May). An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations. Paper presented at the Proceedings of the European Information Security Multi-Conference (EISMC 2013), Lisbon, Portugal.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The Influence of Organisational Information Security Culture on Cybersecurity Decision Making. Journal of Cognitive Engineering and Decision Making: Special Issue on Cybersecurity Decision Making, 9(2), 117-129.

Pattinson, M., & Anderson, G. (2004, 26 November). Risk Homeostasis as a Factor of Information Security. Paper presented at the 2nd Australian Security Management Conference, Perth, Western Australia.

Pattinson, M., & Anderson, G. (2007, April). End-user risk-taking behaviour: An application of the IMB model. Paper presented at the Proceedings of the 6th Annual Security Conference, Las Vegas, Nevada, USA.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Jerram, C. (2015). Examining attitudes toward information security behaviour using mixed methods. Paper presented at the Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), Mytilene, Greece.

Pricewaterhouse Coopers (PWC). (2014). Defending Yesterday -- Key Findings From The Global State of Information Security Survey 2014.

Pricewaterhouse Coopers (PWC). (2015). Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.

QSR International. (2012). NVivo 10 [Computer Software], Version 10.

Schneier, B. (2004). Secrets and lies: digital security in a networked world: Wiley.

Schultz, E. (2005). The human factor in security. Computers & Security, 24(6), 425-426.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.

Telstra. (2014). Telstra Cyber Security Report 2014: Security Insights, Trends and Impact to Australian Organisations: Telstra.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

Wilde, G. J. S. (2001). Target Risk 2: A New Psychology of Safety and Health. Toronto: PDE Publications.

Wood, C. C., & Banks, W. W. (1993). Human error: an overlooked but significant information security problem. Computers & Security, 12(1), 51-60.