Theorising on risk homeostasis in the context of information security behaviour

1. Introduction

Modern-day information security cannot be defined or understood as a pure technical problem. Information technology is a commodity that is used by humans and is therefore a function of the combined effect of human and technological aspects. These human factors ultimately determine the success or failure of information security programmes. The statement on the role of humans in information security is nothing new and a large number of research projects dealing with the problem exist (Frangopoulos et al., 2014; Furnell and Clarke, 2012; Parsons et al., 2010). Despite the comprehensive research efforts in this area, there is still no absolute or definitive solution for what seems to be a very basic problem. The privacy paradox (Kokolakis, 2015) or the knowing-doing gap (Cox, 2012a) are good examples of a problem that remains almost a mystery or at least an enigmatic problem. This problem refers specifically to users with a perceived high level of security awareness who also possess sufficient information security knowledge, but who are then easily persuaded to reveal confidential information such as passwords. It is exactly because of the human element in information security that these types of problems occur and persist. Many researchers have acknowledged this and there are a significant number of studies calling for a more holistic approach to information security (Soomro et al., 2016) or attempting to provide new directions and guidelines for behavioural information security research (Crossler et al., 2013).

Several studies related to the behavioural information security problem apply different theories to try and understand human behaviour in the context of information security. Lebek et al. (2013) reported that a literature review had indicated that at least 54 different theories have been identified that were applied in the area of information security awareness and behaviour. Of these, the primary behavioural theories (based on the number of publications) are the theory of reasoned action (TRA); the theory of planned behaviour (TPB); the general deterrence theory (GDT); and the protection motivation theory (PMT).

The TRA framework deals with a user's behavioural intention and its two associated components, namely attitude and subjective norm (Gundu and Flowerday, 2013). This framework is often combined with or integrated into other theories and then used to explain aspects of information security awareness (Gundu and Flowerday, 2013; Khan et al., 2011) or information security policy compliance (Siponen et al., 2007). The TPB is an extension of TRA and suggests that individual behaviour is influenced by attitude, subjective norms and perceived behavioural control – the latter being the perceived ease or difficulty in performing a particular behaviour (Ifinedo, 2012). This theory has also been widely applied in information security and includes studies that are linked mainly to information security policy compliance (Bulgurcu et al., 2010; Ifinedo, 2012; Kim et al., 2014; Sommestad and Hallberg, 2013). The rationale for GDT is that people will respond to security countermeasures and the associated severity of punishment for a security violation. Straub (1990) applied this theory and surveyed 1 211 organisations, concluding that security countermeasures that include deterrent procedures result in lower computer abuse. Other examples where GDT or variations thereof were applied can be found in D'Arcy et al. (2008), Siponen et al. (2007) and Vaidyanathan and Berhanu (2012). PMT is another psychological theory that was originally developed within a framework of fear-arousing communication (Boer and Seydel, 1996). The theory is often used to predict behaviour and is based on two cognitive processes, namely threat appraisal

and coping appraisal (Jansen, 2015). Threat appraisal is composed of a perceived vulnerability and a perceived severity component, whereas coping appraisal consists of elements such as self-efficacy, response efficacy and response cost (Ifinedo, 2012). PMT has been applied in a number of information security behaviour studies and was found to be useful to predict security behaviour (Crossler, 2010; Herath and Rao, 2009a; Ifinedo, 2012; Jansen, 2015; Meso et al., 2013; Vance et al., 2012).

Behavioural theories on their own do not always provide sufficient answers to information security behaviour problems. As mentioned, the theories are often combined in an effort to obtain new insights into security problems. Also associated with these psychological theories are a large number of other human-related aspects that may be utilised to influence change in behaviour. An example of one factor that is strongly linked to the theories highlighted above is fear. Fear is regularly used as a persuasion technique to change behaviour (Bada and Sasse, 2014) and is also a driver of the PMT framework (Crossler et al, 2013). Closely related to fear is the role of penalties as an enabler for change in security behaviour (Herath and Rao, 2009b). Other interesting factors that may influence a user's perception of risk and information security are the availability heuristic, optimism bias, omission bias et cetera (Parsons et al, 2010). The role of these and other cognitive biases has also been studied by other researchers (Tsohou et al., 2015).

Despite all the comprehensive and well-researched theories, models and factors that influence information security behaviour, it may take only one simple phishing test to prove that there are still significant and perhaps serious challenges in the security behaviour arena – an example of such a phishing test can be found in Kearney and Kruger (2013). With this brief mention of the more prominent theories and influential factors in mind, the ensuing paper theorises on risk homeostasis as a relevant factor (or possible theory) in information security and subsequently discusses one or two other relevant options that may be associated with information security and the theories surrounding it. The study is guided by a primary research question that asks whether the understudied risk homeostasis theory (in the context of information security) may offer any new insights into the paradoxical information security behaviour of users.

The remainder of the paper is organised as follows: The next section provides a short background or motivation for considering a theoretical contemplation of risk homeostasis as a factor in information security. This will be followed by an overview of risk homeostasis and how it relates to information security. The penultimate section will then focus on some further ideas in the context of information security. Concluding remarks are presented in the final section.

2. Motivational background

The significant role that the human element plays in information security means that information security behaviour cannot be understood completely by relying only on human data that are normally obtained from surveys and other measuring instruments. Doing this turns a complex human-scientific problem into a data-driven science that may present a whole new host of problems.

Consider a situation in which respondents are asked to write down the most important risk to privacy. Based on the results (and usually a few statistical tests) it would be possible to state that the number one risk to privacy is risk *x*. It seems fair to say that some valuable learning has taken place and that decision-makers are now better informed to make more appropriate human security decisions. However, we are no closer to a greater understanding of anything and the results are far from a generalisation of users and their perception of risk. A response to the same question may be entirely

different the next day, week or year. Circumstances, perceptions, technology et cetera change over time and differ from one organisation to the next. This makes the initial results valid for only a short and undetermined period of time. In addition to this, Roghanizad and Neufeld (2015) state that decisions entailing risk are reliant on a user's non-rational, gut-level intuition – a clear indication that responses cannot and should not be generalised. A survey, measuring or even observations are acceptable, but the methodology of these techniques is aimed at generating more data which in themselves offer no or very little explanation or understanding of information security behaviour – they provide lists, catalogues and classifications (Fricke, 2015).

Statistical tests that are frequently used with surveys and questionnaires present their own unique problems and Fricke (2015) lists, with supporting literature sources, a number of common errors in statistical analysis. These techniques and their associated errors are regularly employed in information security studies and include null hypothesis significance testing, stepwise regression, multiple comparisons, subsetting, overfitting, univariate screening and dichotomising continuous variables. Also in the context of information security, Frangopoulos et al. (2014) warn against the problem of respondents being biased when completing questionnaires. They refer to social desirability (responding in a way that is socially acceptable) as one of the problems that is also confirmed by other information security researchers (Crossler et al., 2013). A survey on previous work on quantitative representation and analysis of information security shows that the validity of most of these methods is unclear and, based on this, it is then concluded that quantified security is a "weak hypothesis" (Verendel, 2009). Methodological challenges in quantitative empirical research are also recorded from time to time in other IT-related studies (Vehovar et al., 2006).

The above arguments are by no means an objection to surveys, questionnaires or generating data pertaining to information security behaviour. These techniques do have advantages such as the continuous assessment of security-related outcomes; their usefulness in testing theories; and the fact that it is an easy way to get access to larger sample sizes. However, to be able to make new discoveries in information security behaviour that is beyond a dataset and the inductivism that goes with it, more theories, thoughts and problems are needed. This is exactly why, to a certain extent, researchers investigate psychological theories such as those mentioned in the introduction.

There are also other theories that need to be considered in the context of information security behaviour. Examples include the well-known risk homeostasis theory that was introduced by Wilde (1994); theories on users who suffer from security fatigue (Furnell and Thomson, 2009); the theory of narcissism in organisations (Cox, 2012b); and the so called "slower is faster" theory (Gershenson and Helbing, 2015). Some of these theories have already been touched on in an information security context but need to be explored in more depth, as it appears that they are able to offer some conceptual explanations without relying too much on data that have been obtained from questionnaires. Risk homeostasis is one of the theories that has been associated with information security a number of times (Pattinson and Anderson, 2004; Stewart, 2004). In the next section, risk homeostasis will be investigated theoretically as a model that may assist in understanding some of the recurring information security behaviour problems. It will be argued, amongst other things, that there may be certain commonalities between risk homeostasis and other theories such as the PMT framework that has been mentioned earlier. If there are indeed links between the two frameworks, the large number of studies on PMT certainly warrants a closer look to risk homeostasis and it may be worthwhile to at least start theorising on the risk homeostasis theory and what it may offer to information security.

3. The theory of risk homeostasis

It is clear from the literature that the different behavioural theories that have been mentioned in the introduction are popular and well-researched topics in information security. The risk homeostasis theory, however, seems to be a topic that is not one of the current focus points in information security. Very few resources on studies exist in which risk homeostasis is treated as a factor or an influential theory in information security. Pattinson and Anderson (2004) have performed an introductory study of risk homeostasis as a factor in information security, but other researchers only briefly mention the theory as a possible explanatory tool (Albrechtsen and Hovden, 2009; Parsons et al., 2010).

3.1 Risk homeostasis explained

Risk homeostasis is a risk compensation or behavioural adaptation theory that was introduced by Wilde (1994, 2001). According to the theory, people will accept a certain level of risk until the situation changes, for example by introducing new or additional safety measures. People will then change their behaviour to compensate for a change in risk levels. Parsons et al. (2010) state succinctly that "if conditions are perceived to be less risky, then people may take more risk, and if the conditions are perceived to be more risky, then the amount of risk taken may be reduced". Wilde (2001) explains the theory by using a thermostatic control model that continuously changes to maintain a desired temperature. The theory was primarily developed and demonstrated in the area of road safety with the 1967 Sweden change from left-hand to right-hand traffic (Wilde, 1998) and the accident rate per head of a population (Wilde, 2001) as representative examples. Application of the theory is not just limited to road safety and similar examples, though; it can be found in the medical field where vaccination, for example, may encourage promiscuity (Brewer et al., 2007; Pinkerton, 2001). The homeostatic model that has been suggested by Wilde is depicted in Figure 1 with some minor word changes to reflect an information security environment.

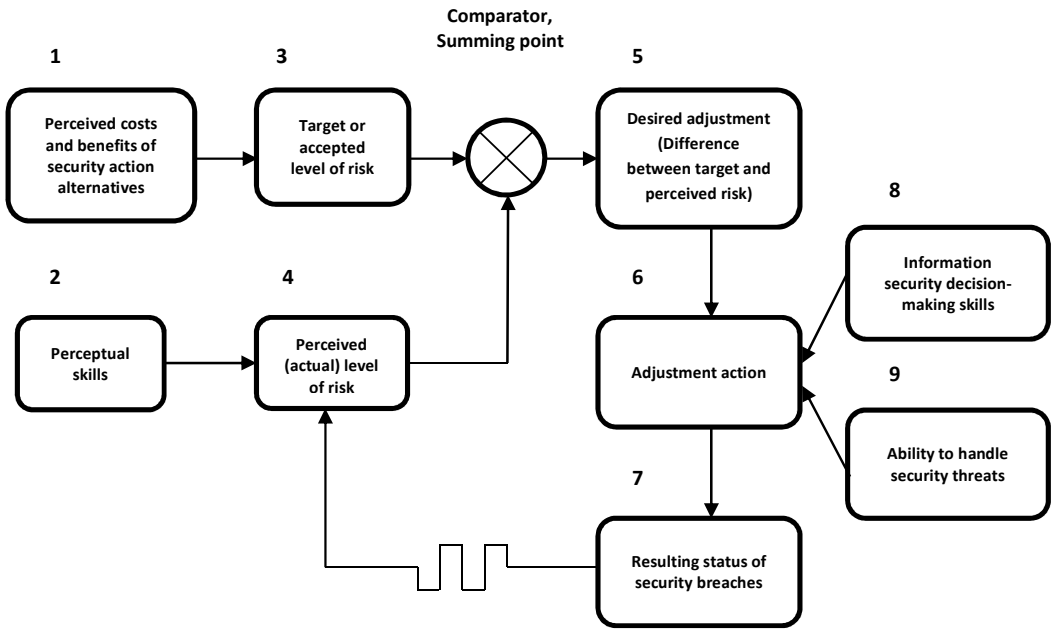

Figure 1: Risk homeostasis model, adapted from Wilde (2001)

The principles of the model in Figure 1 can be summarised in the context of information security as follows:

A user may determine a preferred or target level of risk (box 3), based on factors such as experience, information security training and awareness programmes, cultural factors and social factors (box 1). Wilde (2001) argues that this target level of risk is specifically determined by four categories of motivating (subjective utility) factors, namely the expected *advantages* of comparatively *risky* behaviour alternatives (e.g. saving time by ignoring a security measure); the expected *costs* of comparatively *risky* behaviour alternatives (e.g. time and effort to recover from a computer virus); the expected *benefits* of comparatively *safe* behaviour alternatives (e.g. maintaining the confidentiality, integrity and availability of information); and the expected *costs* of comparatively *safe* behaviour alternatives (e.g. cumbersome procedures). Based on these four categories, it is then concluded that if the expected advantage of risky behaviour (category 1) and the expected costs of save behaviour (category 4) are high, the target level of risk will also be high. Conversely, the target level of risk will be low if the expected costs of risky behaviour (category 2) and the expected benefits of safe behaviour (category 3) are high. Any significant information-security-related event will cause a change in the perceived level of risk (box 4). If new security measures are implemented, for example, or if new security threats emerge, the perceived level of risk will be lower or higher accordingly. This change means that the perceived risk has become notably different (lower or higher) than the target level of risk. In the case of a new threat, users tend to change their security behaviour by choosing more secure alternative options (box 6). This, in turn, will result in a change of status (rate) of security breaches (box 7). As time passes and users become more informed about the new threat, they may realise that the threat is not that serious, or they may discover that the new threat is well controlled through new security measures, or they may simply become used to the new threat. The level of perceived risk may then drop below the target risk and users may start to behave less cautiously, which will then result in a new surge in the number of security breaches. A risk homeostasis model is therefore a closed loop of processes and variables that are continuously adjusted and does not imply constancy. It should thus be seen as a process and not an outcome (Wilde, 2001). The homeostasis process operates on the level of individuals, but Wilde also argues that individuals collectively represent larger groups or populations of people.

It is noteworthy that the risk homeostasis theory is not free from negative critique and there are researchers who do not agree with the theory. O'Neill and Williams (1998) present a rather sarcastic rebuttal of the theory and reject it as a mere hypothesis. Their arguments are based on road safety examples and may be debatable. Trimpop (1996) provides further details and literature references on arguments for and against risk homeostasis.

3.2 Risk homeostasis in information security

Surprisingly, there is very little in the literature on risk homeostasis in the context of information security. Pattinson and Anderson (2004) believe that risk homeostasis applies to many information security scenarios. According to them, risk homeostasis is a management theory and the essence of information security is to manage risk. To demonstrate its applicability, they describe a few practical (hypothetical) examples that include firewalls and anti-virus software, the introduction of a new security-related policy, physical security and the use of specific software controls. Based on these examples, they then conclude that there may be a number of advantages for organisations if they recognise risk homeostasis as a valid component of information security risk. Stewart (2004) also contends that risk homeostasis is a factor in information security and presents new directions for security professionals, companies and the security industry on how to treat risk. Risk homeostasis theory in the context of information security was also referred to in a study by Sawyer et al. (1999). In this research report, the authors studied the role of risk homeostasis in response to the well-known Michelangelo computer virus threat and concluded that risk homeostasis does indeed play a role in

risk perceptions, risky behaviours and protective behaviours. Other researchers mention risk homeostasis only briefly as a possible tool for explaining risk issues in information security. Examples include Farahmand et al. (2008), who presented risk homeostasis as background information in their study on incentives and perceptions of information security risks; Pattinson and Anderson (2007), who listed the theory of risk homeostasis as one of the human factors that will impact upon an organisation's information security environment; Albrechtsen (2007), who suggested risk homeostasis theory as an explanation for poor security behaviour of users and, based on this, concluded that new approaches are needed to manage the role of users in information security; and D'Arcy and Green (2014), who noted an unexpected negative association between perceived organisational support and security compliance intention. They posited that the explanation for this observation is related to the concept of risk homeostasis, as employees who perceive strong organisational support in general may feel that information security problems will be handled by the IT department and that compliance practices are therefore not critical. Studies also exist where the focus is on different (but related) topics, but where the risk homeostasis theory is mentioned, for example in a study of Williams and Noyes (2007) on perceptions of risk in decision-making, and in a study of Workman et al. (2008), who constructed a threat control model to understand the knowing-doing gap of users.

One of the problems of accepting the risk homeostasis theory in the context of information security is the difficulty in determining the extent of its application (Pattinson and Anderson, 2004). The use of a repertory grid technique to try and measure risk-taking behaviour has been proposed by Pattinson and Anderson (2004), whereas Hoyes et al. (1996) list four approaches to evaluate the claims of risk homeostasis. These four approaches are the construction of theoretical/cognitive and mathematical models; the examination of loss statistics; the performance of experiments in which measures are taken before and after an intervention; and simulation studies. It is important to note that all these proposed methodologies have their own unique shortcomings and may not be suitable in all circumstances. What is significant, though, is that the mechanism in risk homeostasis (to adjust or regulate risk) involves three behavioural changes, namely behavioural adjustments within the environment (to do the same thing but in a different manner); "mode migration" (to stop doing something and to do something else in order to achieve the same objective); and avoidance (to stop doing something) (Hoyes et al., 1996).

In an effort to demonstrate (not to prove) the possible presence of homeostatic principles in information security behaviour, the ensuing paragraphs of this section refer to case studies that were conducted earlier and that have already been reported on in the literature (Kearney and Kruger, 2013; 2014). The case studies entail practical information security exercises that were conducted at a very large utility company with over 3,500 IT users. The company has an in-house information security training programme that is mandatory for all staff with access to the IT infrastructure. The main objective of this programme is to make IT users aware of information security threats and risks, as well as to explain to them their responsibilities and role in protecting the company's information assets. There are also a variety of formal and informal channels to inform users on an on-going basis of the importance of information security and its associated risks. Top management views information security as a vital function and promotes its support for a strong and secure information environment publicly. All of these are indicators that a high level of information security awareness is maintained in the company. The high level of information security awareness is further confirmed by formal (e.g. internal audits) and informal (e.g. conversations, newsletters and seminars) activities in various sections of the company. It is therefore reasonable to assume that IT workers in the company under

study are well informed about information security, the associated risks and threats and how to react or respond to them.

Against this background of a high level of information security awareness, a practical phishing experiment was conducted in which users were asked (via email) to provide their usernames and passwords on a web link. The results were unexpected and contradictory to the high levels of security awareness; of the 280 users who responded over a short period of time, 231 (83%) revealed the required personal details. Complete details of the phishing exercise were reported in Kearney and Kruger (2013). This test was later on followed up with a similar phishing test and results showed that there was no improvement in terms of the number of people who gave away their personal details; in fact, the numbers increased from the first to the second test. Detailed results on this follow-up test were presented in Kearney and Kruger (2014).

In an effort to understand the observed security behaviour better, a trust survey was conducted (Kearney and Kruger, 2014). The aim of the trust survey that was carried out on an interview basis was to determine whether trust plays a role in information security behaviour. A secondary objective was to obtain specific information on how users perceive risks and controls pertaining to email and social engineering threats. Results of the trust survey have shown that there is a significant high level of trust amongst employees in the ability of the company to provide a safe, secure and trustworthy environment. Without exception, responses to questions such as "Do you think the organisation protects and secures email communications and related data adequately?" were all positive. A significant number of respondents also indicated that they prefer to do their home banking and other online transactions from work as they feel protected and safe in the work IT environment. Further significant and insightful information was obtained (and confirmed) during follow-up informal discussions with some of the respondents. Explanations on why certain actions are normally taken, including aspects such as workload, limited time to complete tasks, trust and experience of well-controlled risk areas, were given by a large number of respondents.

Based on the results of these practical tests, it appears as if risk homeostatic principles do play a role in information security behaviour. When employees, for example, know or perceive that adequate controls are in place, they will adjust their risk exposure upwards. Users may become more careless and respond to the phishing scam when they know (or perceive) that adequate controls (e.g. spam filters) are in place. The observed high level of trust and associated high number of phishing victims are in line with the risk homeostasis concept, that is, the high level of trust (and thus the low level of risk experienced by users) apparently leads to users compensating for low risk by changing their behaviour and taking more risks, eventually becoming victims of a security breach such as the phishing test. Furthermore, circumstances and feedback that has been received fit perfectly into the motivating factors that Wilde (2001) claims to be determinants of the target level of risk (see section 3.1). The advantage of risky behaviour that is fuelled by the high level of trust is fairly high – this is evidenced by remarks of respondents such as "I have a high workload" (and thus no time for random small problems); "I need to complete certain tasks"; and "I do not have time for cumbersome procedures to investigate or report emails". These issues make it much more attractive to choose the riskier option of providing the required details. It is also a fact that the cost of safe behaviour is high. If a user wants to investigate or report the incident, it will take time – something that users are not prepared to give up easily. Users confirmed that they trust and have experience of good controls; this contributes to an attitude of "no need for concern". The high levels of these two motivating factors will drive the target risk that users are willing to take higher, whereas the perceived risk is low; this, in turn, will result in riskier behaviour such as falling for a phishing scam. It may be argued that users can simply ignore the phishing email, which is the correct thing to do. However, the high levels of

trust, coupled with a perceived safe and secure environment, cause many users to believe that if they do receive an email, it will be a legitimate message to which they should respond – a typical homeostatic assumption.

The real world example described here does not prove that risk homeostasis is present in each and every security incident. It is a practical test and observation that support the homeostatic arguments of other researchers and provide new insights into security behaviour. More importantly, it opens up new and exciting avenues that can be explored (together with other psychological models) to explain the sometimes paradoxical information security behaviour.

3.3 Risk homeostasis: similarities with other models

As mentioned in the introduction, the use of psychological and other cognitive models in information security has almost become a de facto standard. Some of the more prominent models and their application were briefly discussed in the introduction. Additional support for this type of approach in information security can also be found in other more generic studies of researchers such as Anderson and Moore (2009), Enrici et al. (2010) and Tsohou et al. (2015).

Risk homeostasis is also considered a behavioural framework that tries to explain behaviour in terms of risk and there are many conspicuous similarities between risk homeostasis and the other prominent behaviour models. Given the popularity of these other models and approaches in information security behaviour, it is noteworthy that there is a considerable lack of studies on risk homeostasis as a potential explanatory theory for information security behaviour. The rationale of this section is therefore to highlight some of the similarities between risk homeostasis and other well-studied behavioural models briefly. The idea is to show the need for more focused risk homeostasis studies in the context of information security.

The theory of reasoned action (TRA) and its extension, the theory of planned behaviour (TPB), are mainly based on users' intention which is driven by their attitude towards security behaviour. Bulgurcu et al. (2010) have drawn on the TPB model and state that attitude is influenced by *benefit of compliance, cost of compliance* and *cost of non-compliance*. Wilde's (2001) motivating factors in risk homeostasis are also significantly influenced by attitudes and perceived behavioural control. The statements by Bulgurcu et al. (2010) may therefore also be stated in terms of the motivating factors in risk homeostasis, for example the *benefit of safe behaviour (compliance)*, *cost of safe behaviour (compliance)* and *cost of risky behaviour (non-compliance)*.

There also seems to be an "overlap" amongst concepts in protection motivation theory (PMT) and the motivating factors in risk homeostasis. Ifinedo (2012) explains that PMT consists of two distinct processes called a threat appraisal and a coping appraisal. Part of the threat appraisal is an evaluation of the perceived severity, in other words the severity of the consequences of the event, for example non-compliance (behaviour) with a security policy. This is an analogous statement of Wilde's motivating factors where the advantages and costs of behaviour are weighed. The coping appraisal process consists of elements such as response efficacy (the belief about the perceived benefits of the action taken) and response cost (the perceived opportunity cost adopting a recommended behaviour). Again, these elements translate seemingly easy into the motivating factors of risk homeostasis.

Other theories such as the general deterrence theory (GDT) and the closely related factor of fear are also related to the motivating factors, as an emotion such as fear will influence a user's decision on expected cost benefits of a safe or risky behaviour option. This is confirmed by Johnston and

Warkentin (2010) who concluded that fear appeals do impact end user behavioural intentions to comply with recommended individual acts of security.

The aim of this summarised section is not to provide a comparative analysis of risk homeostasis with other well-known behavioural models, but rather to point out that all these models have similarities and are, to a certain degree, in one way or another linked to each other. It therefore seems that if the (other) psychological models are frequently studied in the context of information security, the seemingly associated risk homeostasis theory will probably also provide new insights and explanations to the recurring information security problems that are linked to the human element in information security.

4. Discussion and concluding remarks

Risk homeostasis on its own cannot provide absolute answers to information security behaviour. Shameli-Sendi et al. (2016) rightly pointed out that risk is also dependent on other factors that are constantly changing. These other factors will influence the perceived benefits and costs of a chosen behaviour. One example is the personal trait of narcissism that will influence perceptions and behaviour. Narcissism is described by Campbell et al. (2011) as a stable individual difference consisting of grandiosity, self-love and inflated self-views but except for the work of Cox (2012a, 2012b), there is very little on narcissism and information security in the literature.

The objective of the brief discussion of risk homeostasis in this paper is to highlight the opportunity to further theorise on information security risks, behaviour and a possible model that can help in explaining these intricacies. Security specialists and decision-makers will have to acknowledge that risk is not really quantifiable and that the evaluation of multiple risk factors pertaining to the human aspects of information security is only subjective. Due to the overwhelming human aspects and the many influencing factors, it is also necessary to accept that information security no longer operates in a paradigm of order where it is assumed that all phenomena are context-free; what is needed is a multi-level understanding of information security and the environment in which it operates. Stewart (2004) clearly explains the difference between another control measure and the creating of an environment in which users understand risks. According to his explanation, Western Australia passed a law in 1992 that made the wearing of a safety helmet for cyclers compulsory. However, the number of fatalities remained more or less on the same level after the law was passed. In the Netherlands, with more cyclists and only a few of them wearing helmets, the fatality and injury rates were much lower. The difference, according to Stewart, is that Australia identified a risk and implemented a control, whereas the Netherlands created an environment in which cyclists (users) could understand the risks and implemented new strategies (e.g. dedicated cycle lanes) to deal with the problem.

In general, the acceptance of a risk homeostasis model implies two important concepts to be dealt with, namely monitoring and intervention. It is important that a monitoring system is implemented to determine whether risk homeostasis principles are present and whether target and actual risk levels are appropriately evaluated. A natural starting point in the management and monitoring of information security risks is to ensure that the expectations of different groups of people are well managed. One way to do this is to assess the level of possible perceptual differences, which may give an indication of differences in the perceived and target levels of risk. Measuring techniques to achieve this are well documented in the literature (Ackam et al., 2015; Albrechtsen and Hovden, 2009; Posey et al., 2014). Another tool is trust surveys that may be employed to identify the presence of homeostatic activities. In section 3.2, an example of such a trust survey and the way in which it may be linked to risk homeostasis have been presented. Furthermore, certain practical, information security-related tests

may be used to reveal information on risk levels and a need for intervention. An example of a practical security test is a phishing exercise – also briefly described in section 3.2. These types of security tests will provide valuable insights into risk levels of a risk homeostasis model and are also well documented in the literature (Jansson and Von Solms, 2013; Pattinson et al., 2012). Finally, more direct and intensive investigations into different cost/benefit scenarios may be performed to monitor and evaluate risks in a risk homeostasis model. Beautement et al. (2008) have conducted an informative study in this regard that can be translated directly to the principles of a risk homeostasis model. In this study, examples of specific scenarios of cost/benefit perceptions that were evaluated through user interviews are presented. Examples of such practical scenarios and monitoring opportunities documented by Beautement et al. include the cost or benefits of centrally scheduled tasks (e.g., automated virus scans); additional authentication; use of encryption; and restrictive firewalls.

In addition to the monitoring aspect, the risk homeostasis theory also suggests that interventions (usually technology, new policies or new awareness campaigns) be implemented to adjust perceived risk levels. A major issue with this, again, is the link between the human aspects and the interventions. In his recommendations, Stewart (2004) posits that this is frustrating for users, especially when users believe that the level of security is sufficient. This implies that whenever risk homeostasis is considered as a model for managing risk, special attention should be given to the way in which risks and awareness are presented to users. Security measures may sometimes be perceived as being an obstacle and are then simply ignored (Bada and Sasse, 2014). In other cases, security-related information passed on to users may be so overwhelming that users may filter them out mentally as being something similar to spam (Furnell and Thomson, 2009). This important aspect of security fatigue should be taken into account when using the risk homeostasis model to manage risks and security behaviour. Bada and Sasse (2014) refer to the security versus usability triangle and argue that security fatigue will become an issue if security and usability are not balanced. The two concepts tend to be inversely related and a high secure system with low usability will result in a secure system that no one uses, whereas a low secure system with high usability will be used by everyone, including unauthorised users. Security fatigue is a real threat in general, but also specifically in the risk homeostasis model when the aim is to change perceptions of users. Furnell and Thomson (2009) offer guidelines on security fatigue factors that include effort (the requirement to comply); difficulty (ease in providing the required effort); and importance (way in which a user prioritise the need to secure an asset).

When considering security fatigue and security measures, Norman (2010) makes the following statement: “The more secure you make something, the less secure it becomes”. This is an issue that should be considered seriously by security specialists. A possible framework to understand this contradictory principle that has not yet been applied in an information security context is the *slower is faster* (SIF) effect that has been described by Gershenson and Helbing (2015). The basic premise behind the SIF effect is that a system performs worse when the components of the system are trying to do better. Gershenson and Helbing present various examples to illustrate this effect. Some of the examples include pedestrian dynamics (individuals trying to evacuate a room too quickly, leading to clogging and a reduced outflow as opposed to a calmer and slower evacuation), vehicle traffic, social dynamics, ecological systems, logistics and supply chains. The most probable message from the SIF effect to information security is that security awareness programmes need to contain selective material and should not be bombarding users with overwhelming amounts of security information that may ultimately result in less security.

Presenting less (security) information to achieve better (security) behaviour appears to be viable. Bargh et al. (1996) performed interesting experiments to show that behaviour is often triggered automatically in the mere presence of relevant situational factors. In one of these experiments, participants were asked to construct short sentences from a few scrambled words. The authors used three versions of the scrambled-sentence test with the first one being intended to prime the construct *rude* (using words such as aggressive, annoying, interrupt and infringe); the next one intended to prime the construct *polite* (using words such as respect, cordial and courteous); and the last one intended to prime a *neutral* condition. Once a participant had constructed the sentences in one of the three categories, he/she was asked to proceed to the next room in order to receive further instructions. In this room, the instructor was talking to another person, causing the arriving participant to wait. The time taken before the arriving participant would interrupt them was recorded and the interesting and surprising results were that those who were exposed to "rude" words would interrupt them quicker than those who were exposed to "neutral" words. The participants exposed to "polite" words would wait the longest before they would interrupt. Using the results of this automaticity of social behaviour experiment, the question for information security specialists is the following: Would it not be more advantageous to have a security awareness programme (or whatever is used to try and influence behaviour) that focuses on "short" pieces of information rather than the traditional "longer" security and awareness programmes? This approach will not only influence behaviour but will also serve as a counter measure for security fatigue. It also fits in perfectly with the SIF effect.

To further illustrate the potential problem of too much security information and too many controls, a small practical test was conducted by using a non-probability convenience sampling method. These types of sampling methods provide a quick and easy way to poll the opinion of people (Wegner, 1993). Twenty five fourth-year students in Computer Science were asked to express what their preference was between two different instructions on how to choose a password. The first option simply states, "Choose and manage your password in a safe and secure manner to ensure that it stays confidential at all times". The second option also instructs them to choose a password and then presents a list of 14 properties of a safe password (e.g. length, characters to use etc.) that respondents have to comply with. A total of 18 students responded and 50% of them indicated that they would prefer the shorter instruction in the first option. Comments on why they chose the shorter instruction include the following: "I know the importance of passwords"; "Too many instructions will lead to people not worrying anymore"; and "Too many rules are irritating". It should be noted that these respondents were students who had not yet entered the work place and had not yet been exposed to formal information security training and awareness programmes. Despite these facts, they already showed a preference for shorter or easier security messages – and maybe they already suffered from security fatigue, albeit to a lesser extent.

To summarise: Risk homeostasis offers to decision-makers a different (and not sufficiently explored) way of understanding and managing risk and information security behaviour. The homeostatic principle of interventions to adjust perceived and target risk may cause other difficulties of which security fatigue appears to be an important role player. The potential problems associated with security fatigue may, however, be addressed with other sociological approaches such as the slower is faster (SIF) effect and the automaticity of social behaviour experiments that complement each other.

5. Conclusion

The human aspect of information security has turned it into a complex area of study. There is widespread recognition of the fact that technology on its own does no longer offer complete solutions to the information security problem. New models, approaches and techniques are needed to manage

and understand information security risks and behaviour. What seems to be popular amongst security specialists is to investigate and apply behavioural theories that originate from the psychological and social sciences. One such theory that appears to be almost ignored in the context of information security is the theory of risk homeostasis. Some information security researchers have touched on this theory (Farahmad et al., 2008; Pattinson and Anderson, 2004; Stewart, 2004), but there is a general lack of literature on risk homeostasis in information security. This paper attempts to create an opportunity to begin theorising on risk homeostasis as a model that should be considered, along with other factors, in information security frameworks.

The paper suggests that risk homeostasis offers a different view and way of understanding security behaviour. A brief motivation on why risk homeostasis should be considered was followed by a description of the theory. The model's applicability to information security was explained and similarities with other behavioural frameworks were highlighted. In the final concluding remarks, it was also pointed out that there are two issues attached to the adoption of a risk homeostasis model – a need for a monitoring function as well as a need to implement specific interventions to adjust perceived risk levels. Linked to these two issues are specific difficulties, of which security fatigue is a major role player that may occur when applying the homeostatic principles. Suggestions to deal with this problem were made and include approaches that have not yet been implemented in information security – the two approaches that were suggested are the slower is faster (SIF) effect and an automaticity of social behaviour assumption.

In general, the paper opens up the prospect to theorise on the risk homeostasis concept in information security behaviour and culture. At a more practical level, it offers decision-makers and security specialists useful information and new insights that could be advantageous in a strategic security planning process.

References

Akcam, B.K., Hekim, H. and Guler, A. (2015). "Exploring business student perception of information and technology". *Procedia – Social and Behavioral Sciences*, 195:182-191.

Albrechtsen, E. (2007). "A qualitative study of users' view on information security". *Computers & Security*, 26:276-289.

Albrechtsen, E. and Hovden, J. (2009). "The information security digital divide between information security managers and users". *Computers & Security*, 28:476-490.

Anderson, R. and Moore, T. (2009). "Information security: where computer science, economics and psychology meet". *Philosophical Transactions of the Royal Society A*, 367:2717-2727.

Bada, M. and Sasse, A. (2014). "Cyber security awareness campaigns. Why do they fail to change behavior?" Global Cyber Security Capacity Centre: Draft working paper. July 2014.

Bargh, J.A., Chen, M. and Burrows, L. (1996). "Automaticity of social behavior: direct effects of trait construct and stereotype activation on action". *Journal of Personality and Social Psychology*, 71(2):230-244.

Beautement, A., Sasse, M.A. and Wonham, M. (2008). "The compliance budget: Managing security behaviour in organisations". Proceedings of the New Security Paradigms Workshop (NSPW08). DOI: 10.1145/1595676.1595684.

Boer, H. and Seydel, E.R. (1996). "Protection Motivation Theory", available at doc.utwente.nl/34896/1/K465_.pdf (accessed 12 November 2015).

Brewer, N.T., Cuite, L.C., Herrington, J.E. and Weinstein, N.D. (2007). "Risk compensation and vaccination: can getting vaccinated cause people to engage in risky behaviours?" *Annals of Behavioural Medicine*, 34(1):95-98.

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

Campbell, W.K., Hoffman, B.J., Campbell, S.M. and Marchisio, G. (2011). "Narcissism in organizational contexts". *Human Resource Management Review*, 21:268-284.

Cox, J.A. (2012a). "Information systems user security: A structured model of the knowing-doing gap". *Computers in Human Behavior*, 28:1849-1858.

Cox, J.A. (2012b). "Organizational narcissism as a factor in information security: a structured model of the user knowing-doing gap". PhD Dissertation, Capella University.

Crossler, R.E. (2010). "Protection motivation theory: understanding determinants to backing up personal data". The 43rd Hawai International Conference on System Sciences. DOI: 10.1109/HICSS.2010.306.

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

D'Arcy, J., Hovav, A. and Galletta, D. (2008). "User awareness of security countermeasurers and its impact on information systems misuse: a deterrence approach". *Information Systems Research*. DOI: 10.1287/isre.1070.0160.

D'Arcy, J. and Green, G. (2014). "Security culture and the employment relationship as drivers of employees' security compliance". *Information Management & Computer Security*, 22(5):474-489.

Enrici, I., Ancilli, M. and Lioy, A. (2010). "A psychological approach to information technology security". 3rd International Conference on Human System Interaction, HSI2010. DOI: 10.1109/HIS.2010.5514528.

Farahmand, F., Atallah, M. and Konsynski, B. (2008). "Incentives and perceptions of information security risks". Proceedings of the 29th International Conference on Information Systems (ICIS). Available at http://aisel.aisnet.org/icis2008/25 (accessed 13 June 2016).

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M. (2014). "Human aspects of information insurance: a questionnaire-based quantitative approach to assessment". Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014).

Fricke, M. (2015). "Big data and its epistemology". *Journal of the Association for Information Science and Technology*, 66(4):651-661.

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

Furnell, S. and Thomson, K. (2009). "Recognising and addressing security fatigue". *Computer Fraud & Security*, 11:7-11.

Gershenson, C. and Helbing, D. (2015). "When slower is faster". *Complexity*, 21(2):9-15.

Gundu, T. and Flowerday, S.V. (2013). "Ignorance to awareness: towards an information security awareness process". *South African Institute of Electrical Engineers*, 104(2):69-79.

Herath, T. and Rao, H.R. (2009a). "Protection motivation and deterrence: a framework for security policy compliance in organisations". *European Journal of Information Systems*, 18:106-125.

Herath, T. and Rao, H.R. (2009b). "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness". *Decision Support Systems*, 47(2):1546-165.

Hoyes, T.W., Stanton, N.A. and Taylor, R.G. (1996). "Risk homeostasis theory – a study of intrinsic compensation". *Safety Science*, 22(1-3):77-86.

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

Jansen, J. (2015). "Studying safe online banking behavior: a protection motivation theory approach". Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015).

Jansson, K. and Von Solms, R. (2013). "Phishing for phishing awareness". *Behaviour and Information Technology*, 32(6):584-593.

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

Kearney, W.D. and Kruger, H.A. (2013). "Phishing and organizational learning", In SEC2013, IFIP AICT 405, eds. Janczewski, LJ, Wolf, H, Shenoi, S. p379-390.

Kearney, W.D. and Kruger, H.A. (2014). "Considering the influence of human trust in practical social engineering". 13th International Information Security for South Africa Conference (ISSA 2014).

Khan, B., Alghatbar, K.S., Nabi, S.I. and Khan, M.K. (2011). "Effectiveness of information security awareness methods based on psychological theories". *African Journal of Business Management,* 5(26):10862-10868.

Kim, S.H., Yang, K.H. and Park, S. (2014). "An integrative behavioral model of information security policy compliance". *The Scientific World Journal,* available at http://dx.doi.org/10.1155/2014/463870 (accessed 14 May 2015).

Kokolakis, S. (2015). "Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon". *Computers & Security*, In Press.

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013). "Employees' information security awareness and behavior: a literature review". The 46th Hawai International Conference on System Sciences. DOI: 10.1109/HICSS.2013.192.

Meso, P., Ding, Y. and Xu, S. (2013). "Applying protection motivation theory to information security training for college students". *Journal of Privacy and Security*, 9(1):47-67.

Norman, D.A. (2010). "When security gets in the way", available at http://jnd.org/dn.mss/when_security_gets_in_the_way.hmtl (accessed 20 November 2015).

O'Neill, B. and Williams, A. (1998). "Risk homeostasis hypothesis: a rebuttal". *Injury Prevention*, 4:92-93.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010). "Human factors and information security: Individual, culture and security environment". Australia Government, Department of Defence. Command Control, Communications and Intelligence Division, Defense Science and Technology Organisation, Edinburgh, Australia.

Pattinson, M.R. and Anderson, G. (2004). "Risk homeostasis as a factor of information security", available at http://www.igneous.scis.ecu.edu.au (accessed 13 April 2015).

Pattinson, M.R. and Anderson, G. (2007). "How well are information risks being communicated to your computer end-users?". *Information Management & Computer Security*, 15(5):362-371.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A. and Butavicius, M. (2012). "Why do some people manage phishing e-mails better than others?". *Information Management and Computer Security*, 20(1):18-28.

Pinkerton, S.D. (2001). "Sexual risk compensation and HIV/STD transmission: empirical evidence and theoretical considerations". *Risk Analysis*, 21(4):727-736.

Posey, C., Roberts, T.L., Lowry, P.B. and Hightower, R.T. (2014). "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders". *Information and Management,* 51:551-567.

Roghanizad, M.M. and Neufeld, D.J. (2015). "Intuition, risk, and the formation of online trust". *Computers in Human Behavior*, 50:489-498.

Sawyer, J.E., Kernan, M.C., Conlon, D.E. and Garland, H. (1999). "Responses to the Michelangelo computer virus threat: The role of information sources and risk homeostasis theory". *Journal of Applied Social Psychology*, 29(1):23-51.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016). "Taxonomy of information security risk assessment (ISRA)". *Computers & Security*, 57:14-30.

Siponen, M., Pahnila, S. and Mahmood, A. (2007). "Employees' adherence to information security policies: an empirical study", In IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, *eds*. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer). p133-144.

Sommestad, T. and Hallberg, J. (2013). "A review of the theory of planned behavior in the context of information security policy compliance", In SEC2013, IFIP AICT 405, eds. Janczewski, L.J., Wolfe, H.B., Shenoi, S. p257-271.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016). "Information security management needs more holistic approach: a literature review". *International Journal of Information Management*, 36:215-225.

Stewart, A. (2004). "On risk: perception and direction". *Computers & Security*, 23:362-270.

Straub, D.W. (1990). "Effective IS security: an empirical study". *Information Systems Research*, 1(3):255-276.

Trimpop, R.M. (1996). "Risk homeostasis theory: problems of the past and promises for the future". *Safety Science*, 22(1-3):119-130.

Tsohou, A., Karyda, M. and Kokolakis, S. (2015). "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs". *Computers & Security*, 52:128-141.

Vaidyanathan, G. and Berhanu, N. (2012). "Impact of security countermeasurers in organizational information convergence: a theoretical model". *Issues in Information Systems*, 13(2):21-25.

Vance, A., Siponen, M. and Pahnila, S. (2012). "Motivating IS security compliance: Insights from habit and protection motivation theory". *Information and Management*, 49(3-4):190-198.

Vehovar, V., Sicherl, P., Husing, T. and Dolnicar, V. (2006). "Methodological challenges of digital divide measurements". *The Information Society: An International Journal*, 22(5):279-290.

Verendel, V. (2009). "Quantified security is a weak hypothesis. A critical survey of results and assumptions". Proceedings of the 2009 workshop on new security paradigms workshop, ACM Digital Library.

Wegner, T. (1993). *Applied business statistics. Methods and applications*, Juta and Co, Ltd.

Wilde, G.J.S. (1994). *Target risk*. PDE Publications, Toronto, Canada.

Wilde, G.J.S. (1998). "Risk homeostasis: an overview". *Injury Prevention*, 4:89-91.

Wilde, G.J.S. (2001). *Target Risk 2*. PDE Publications, Toronto, Canada.

Williams, D.J. and Noyes, J.M. (2007). "How does our perception of risk influence decision-making? Implications for the design of risk information". *Theoretical Issues in Ergonomics Science*, 8(1):1-35.

Workman, M., Bommer, W.H. and Straub, D. (2008). "Security lapses and the omission of information security measures: A threat control model and empirical test". *Computers in Human Behavior*, 24: 2799-2816.