Risk homeostasis and security fatigue: a case study of data specialists

Anusha Bhana
Jacques Ophoff

Risk Homeostasis and Security Fatigue: A Case Study of Data Specialists

Journal:	*Information and Computer Security*
Manuscript ID	ICS-11-2022-0172
Manuscript Type:	Original Article
Keywords:	Information security, Risk homeostasis theory, Security fatigue, Data specialist

Risk Homeostasis and Security Fatigue: A Case Study of Data Specialists

Abstract

Purpose – Organisations employ a variety of technical, formal, and informal security controls but also rely on employees to safeguard information assets. This relies heavily on compliance and constantly challenges employees to manage security-related risks. The purpose of this research is to explore the homeostatic mechanism proposed by risk homeostasis theory, as well as security fatigue, in an organisational context.

Design/methodology/approach – A case study approach was used to investigate the topic, focusing on data specialists who regularly work with sensitive information assets. Primary data was collected through semi-structured interviews with 12 data specialists in a large financial services company.

Findings – A thematic analysis of the data revealed risk perceptions, behavioural adjustments, and indicators of security fatigue. The findings provide examples of how these concepts manifest in practice and confirm the relevance of risk homeostasis theory in the security domain.

Originality/value – This research illuminates homeostatic mechanisms in an organisational security context. It also illustrates links with security fatigue and how this could further impact risk. Examples and indicators of security fatigue can assist organisations with risk management, creating 'employee-friendly' policies and procedures, choosing appropriate technical security solutions and tailoring security education, training, and awareness activities.

Keywords – Information security; Risk homeostasis theory; Security fatigue; Data specialist

Paper type – Research paper

1. Introduction

Employees can be seen as barriers but also facilitators of information security. However, creating a security-minded workforce is a persistent challenge. When organisations place policies and procedures at the forefront of their security efforts this can have a negative impact on employees. In such environments employees often face an array of complex security requirements which are difficult to understand and satisfy (D'Arcy and Teh, 2019). Such potentially unrealistic demands may even lead to experienced employees, with good technical skills, struggling to keep up.

Confronted with security-related workload and cognitive demand an employee may experience increased psychological stress, leading to a chronic state of exhaustion (Choi *et al.*, 2018). Furthermore, this exhaustion is a core component of fatigue. Faced with information security stress and fatigue, employees may start to use coping behaviours. These behaviours are often analysed in the context of behavioural frameworks (D'Arcy *et al.*, 2014; D'Arcy and Teh, 2019).

It is also argued that fatigue can lead to employees constantly performing cost-benefit calculations, choosing to accept certain risks to achieve important work goals (Sasse, 2015). If countermeasures are implemented to reduce employees' risky behaviours this can lead to a vicious circle: security policies and procedures → employee fatigue → risky behaviour is displayed → additional policies and procedures, etc. (Hatashima *et al.*, 2018). In the context of risk, Wilde (1982, 1998) proposed a homeostatic mechanism which predicts that individuals will weigh the expected benefits of risky behaviour against the costs and determine the level of risk they are willing to accept. The impact of such risk calculations, and subsequent adjustment of actions, is not well understood and can often lead to surprising and counterintuitive consequences.

This research explores how risk homeostasis and security fatigue manifests and affects employees with increased responsibility for sensitive information assets. In particular the focus is on data specialists, who transform raw data into information. Bhana and Ophoff (2022) examined cases of security fatigue amongst data specialists. This paper expands and focuses the discussion on risk perceptions and adjustments in behaviour, in line with risk homeostasis. Understanding these factors could assist organisations with risk management, creating 'employee-friendly' policies and procedures, choosing appropriate technical security solutions and tailoring security education, training, and awareness activities. The research follows a case study approach, focusing on data specialists in a large financial services company. Primary data is collected through semi-structured interviews with 12 participants and analysed using thematic analysis.

The rest of the paper is structured as follows. In Section 2 a literature review provides contextual background on risk homeostasis, security fatigue, and related concepts. This is followed by a description of the research design, including the case organisation and participants in Section 3. In Section 4 the results of the thematic analysis and findings are presented. Section 5 presents a discussion of the findings, in relation to prior literature, follows. Lastly, Section 6 concludes by discussing the limitations of this study, along with opportunities for further research.

2. Literature Review

Risk is a fundamental aspect of our thinking about security and can be seen as *"a measure of the extent to which an entity is threatened by a potential circumstance or event"* (NIST, no date). This is typically linked to the adverse impact that could arise and the likelihood of occurrence. Such rhetoric is frequently used as part of fear appeals in information security campaigns, to motivate compliance with security controls, but with mixed results (e.g., Johnston *et al.*, 2015). Individual biases and heuristics are leveraged when making decisions, and risk perceptions may differ between individuals. It is proposed that risk tolerance and risk aversion are important aspects which adds further complexity and nuance to information security decision making (Warkentin *et al.*, 2018). The theory of risk homeostasis (or risk compensation) has been proposed to explain how individuals will always strive to achieve a state of equilibrium when dealing with risk (Wilde, 1982, 1998).

2.1. Risk Homeostasis Theory

Wilde's (1982, 1998) risk homeostasis theory (RHT) proposes a homeostatic mechanism where individuals will adjust their actions to maintain an accepted level of risk. At any given moment an individual will compare their perceived risk against their target level risk and adjust their behaviour to bridge any incongruity between the two, thus achieving homeostatic equilibrium. A simple analogy is that of a thermostat, where the instrument responds to fluctuations in temperature by adjusting its heating/cooling actions to maintain a constant temperature. On average the temperature will remain constant unless a new target level is set (Wilde, 1998). Another illustration of RHT is trapeze artists who take greater risks when performing with a safety net (Renaud and Warkentin, 2017). In a security context, Parsons *et al.* (2010) proposes that when individuals perceive less risk, they are more likely to take risks, while if conditions are perceived to be riskier such risk-taking behaviour may be reduced.

2.2. RHT in Information Security

RHT has been applied to information security on various occasions. In an early example, Sawyer *et al.* (1999) examined risk perception and behaviour at the appearance of the Michelangelo virus. In line with RHT, individual risk perceptions remained unchanged while population risk over the period was impacted. Further correlations have been drawn between personality traits like conscientiousness, agreeableness, and openness to risk taking behaviour by end-users (Alohali *et al.*, 2018)

Subsequently the argument was made that RHT can be applied in organisations, to explain the phenomena where security measures put in place to manage risk are invalidated by counterintuitive behaviours (Stewart, 2004). Organisational security policies, risk culture, and security communication will impact employee propensity to take risks. This is further influenced by individual demographics like age, gender, and education levels, leading to influencing factors at both individual and organisational levels (Pattinson and Anderson, 2004).

Further research on organisational information security has examined why employees engage in riskier behaviour when there is an increased perceived trust in the organisation's security protocols. It is proposed that employees believe stringent technical measures enforced by the organisation is enough to keep them safe and shifts responsibility away from the employee to the organisation (D'Arcy *et al.*, 2014). Renaud and Warkentin (2017) suggest a few information security behaviours that could be influenced by adjusting actions based on the RHT mechanism. These include clicking links, password choice, data backup, downloading files, smartphone protection, app installation, and web trust. However, it should be noted that Renaud and Warkentin (2017) challenge RHT and question the ability of humans to judge risk objectively and correctly.

RHT has also been adapted in several security-related studies. Kearney and Kruger (2016) claimed that RHT can be leveraged to extend knowledge and insights into contradictory human behaviour. They proposed an adapted risk homeostasis model, applied in the context of information security awareness programs, to provide insight into how the homeostatic principle can be used as an intervention to adjust perceived and target risks, ensuring optimal effectiveness of the campaign. Jardine (2020) examines why the introduction/adoption of cybersecurity technology, in this case commercial antivirus software, may introduce harmful effects and have minimal long-term impact. The construct of information problems is added to RHT to explain counterintuitive security outcomes more accurately.

Efforts to secure systems and reduce risk may come at a detriment to users (e.g., in the usability of a system) and increases the likelihood of security fatigue. It has been suggested that security fatigue can play a role in the effort to dynamically balance risk and security behaviour (Kearney and Kruger, 2016). We examine this phenomenon in more detail in the following section.

2.3. Security Complexity and Fatigue

Employees are regularly reminded about security, for example with daily messages to be cautious while performing any online activity. This hyper vigilance can have a potentially detrimental impact on the individual, resulting in a level of despondency. Over time this manifests as weariness and in this context is described as information security fatigue. According to Furnell (2019, p. 1), *"The term security fatigue recognizes the situation in which users of systems and staff in organizations can tire of dealing with security or encountering messages and warnings in relation to it."*

Although fatigue cannot be empirically measured it may be expressed through several factors, such as effort, difficulty, and importance. Effort is described as the energy spent to achieve compliance. Difficulty describes the quantity of energy expended to provide the required effort. Importance is the priority assigned to the compliance task (Furnell and Thomson, 2009). While fatigue is not a new construct, the appearance of security fatigue has increased in prominence.

Furnell and Thomson (2009) describe this as breaching a threshold; becoming weary and desensitised, where compliance becomes too difficult and burdensome. This is the point security fatigue sets in. Stanton *et al.* (2016) describe fatigue as a reluctance to see or experience any more of something. Security fatigue is one cost that users experience when facing constant security messages, advice, and demands for compliance. This cost often results in what security experts might consider less secure online behaviour. Hatashima *et al.* (2018) describe fatigue as a human experience when faced with multiple external actions to mitigate security risk.

2.4. Managing Security Fatigue

Security fatigue may manifest in several ways. Frequent security decisions, information overload, complexity, and uncertainty may lead to employee stress and consequent information security policy violations (D'Arcy *et al.*, 2014). Oto (2012) proposes that employees will simply stop making unnecessary decisions. Should they choose to make a decision, it will be the simplest option driven by immediate needs. This irrational behaviour is driven by feeling a lack of control and general apathy, which potentially increases stress.

Internal and external stressors deplete cognitive resources triggering fatigue. Security-related stress includes innocuous and common stressors, such as repetitive security tasks, but also more serious events such as security breaches. Events particularly intensifying fatigue are unclear security tasks and requirements contrary to job expectations. Stress and emotional reactions have been shown as predictors of information security policy compliance (D'Arcy and Teh, 2019). Failure by employees to adhere to such policies can cause security risks to the organisation. It is argued that when employees are overwhelmed by security messages and exhausted with the effort required to keep information safe, they are likely to ignore concerns raised by the organisation (Beautement *et al.*, 2008).

To protect information and systems organisations implement measures such as security policies and procedures, as well as security education, training, and awareness to encourage employees to adhere to security practices (Pham *et al.*, 2019). To understand the extent of adherence Beautement *et al.* (2008) introduced the concept of a compliance budget, to be used as one would a financial budget. Here the costs and benefits of security compliance are managed and understood. This constant iterative process takes its toll on the user resulting in the depletion of their compliance budget and security fatigue setting in. However, it is likely that security compliance is a much more complicated phenomenon, stemming from the lived experiences of individuals (Ophoff and Renaud, 2021). Shared viewpoints about security compliance may exist amongst employees, which need to be understood to effectively manage security fatigue.

2.5. Security and Data Specialists

Alohali *et al.* (2018) notes data management as a key component in information security. With the introduction of data protection legislation covering most countries across the world, there is an increased focus on ensuring data safety and compliance. For example, the General Data Protection Regulation (GDPR), a European Union law governing data protection and privacy impacts companies who interact with any personal data from EU citizens. Furthermore, the Protection of Personal Information Act (POPIA) of South Africa aims to govern the process of processing personal information recorded in any format by a responsible party within the country. Thus, multiple pieces of legislation may be applicable at the same time. To comply with legislation organisations must adhere to strict security protocols and processes, since there may be severe penalties for a violation.

Employees responsible for processing data must understand the boundaries within which they are working. Chen and Zhao (2012) outline the data lifecycle as: generation, transfer, use, sharing, storage, archival, and destruction. At each phase data is treated differently to comply with regulation and to ensure its protection. During data generation all personal information collected must be acknowledged by the data owner; during data storage and transfer in addition to encryption, transport protocols must be in place to maintain confidentiality and integrity; during use and sharing data must comply with applicable data protection regulation.

The data journey is managed and administered by data specialists, who are responsible for safekeeping and minimising risk to this data. The result of any security incident and data breach may have severe consequences for an organisation, including reputational and financial impacts (Bruemmer, 2016). This responsibility may weigh heavily on employees and increases the stress placed on those entrusted to secure the data. These employees are mandated to maintain customer trust and credibility by ensuring the safety of personal information.

Data breaches are often at the forefront of security concerns. While measures are put in place to protect data the number of security incidents has not decreased. Securing sensitive information assets within an organisation is therefore a growing and persistent concern. Therefore, it seems relevant to ask how data specialists (as a specific but important subset of organisational employees) think about and manage risk, and how possible experience of security fatigue manifests.

3. Research Design

The core of this study is to explore the human experience. The study of risk tolerance and security fatigue are human experiences and are therefore well-suited to an interpretivist paradigm. Taylor *et al.* (2016) state that an interpretivist paradigm aims to understand how the world is experienced through an individual's lens. This creates a personal reality, often driven by the desire to understand social phenomena through forming meaningful ideas, feelings, and emotions.

To develop a thorough understanding of the topic a case study approach was adopted. The case in this instance refers to a group of employees within an organisation where the topic was studied. Yin (2018) advocates for this strategy when the researcher has no control over the behavioural events and the focus is contemporary.

3.1. Case Organisation and Participants

The case organisation is a large financial services company based in South Africa, with a footprint in the rest of Africa. Leveraging information as an asset has increased in strategic importance for the organisation, and there is core team of dedicated specialists supporting the data function. Key positions were created to drive this initiative, such as Head of Data, Head of Data Governance, and Head of Data Acquisition.

Another significant appointment was the first Chief Information Security Officer (CISO). Alongside this appointment the information security community in the organisation has grown, focusing efforts on ensuring information security compliance. This is a multi-faceted approach which include security awareness campaigns. With the increased pressure for organisational legislative compliance employees are fully aware of information security requirements. The organisation is thus relevant, both in terms of processing large volumes of sensitive information as well as implementing strict security protocols to manage security risks, which could lead to employee security fatigue.

A purposive sampling technique was used to target employees in various data specialist roles with a propensity to experience security fatigue. This approach is often employed when working with a small sample (as in case study research) and allows the researcher to choose cases that are particularly interesting and informative. Demographic information about participants is summarised in Table I.

Table I. Participant demographic information

Code	Gender	Age range	Years in role
P1	Male	30-39	1-3
P2	Female	30-39	1-3
P3	Female	20-29	1-3
P4	Male	30-39	4-9
P5	Male	40-49	10-15
P6	Male	20-29	4-9
P7	Male	60-69	10-15
P8	Male	40-49	10-15
P9	Male	40-49	4-9
P10	Male	30-39	1-3
P11	Female	40-49	10-15
P12	Male	30-39	1-3

Participants in this study represented both technical and business roles, such as Database Administrator, IT Manager, Senior Analyst Programmer, Senior BI Developer, Data Engineer, (Senior) Business Analyst, and BI Manager. Participants included nine males and three females, having extensive experience in mid- to senior-specialist roles. The research was granted ethical clearance from the case organisation, as well as the educational institution of the researchers, prior to data collection.

3.2. Data Collection and Analysis

Data was collected between July 2019 and August 2019. For this study semi-structured interviews were conducted with the 12 participants. Each interview lasted about 40 minutes and followed a consistent format to ensure repeatability across the study (Yin, 2018). The interview session was reflexive in nature, to allow exploratory insights to develop naturally with the progression of the interview. The interview questions are listed in Appendix A.

All interviews were recorded and transcribed for subsequent analysis. Data was captured in the NVivo computer-assisted qualitative data analysis software. Care was taken to ensure the data was fully anonymised and appropriately stored for analysis. Thematic analysis was used to analyse the data and followed the six-step approach recommended by Braun and Clarke (2006), which allowed the discovery of themes and patterns in the data.

4. Analysis and Findings

This section presents the themes that emerged from the thematic analysis. This is structured into three broad categories: risk perceptions; behavioural adjustments; and indicators of security fatigue.

4.1. Risk Perceptions

The participants have access to highly confidential information, including customer banking details, income details, medical history, and contact information. When asked about the level of comfort they have with access to such information, the general feeling is one of ease. Participants appeared desensitised to the highly sensitive nature of the information they have access to. They are familiar with the information and do not perceive any risks in having access to it.

A level of unease sets in when participants are called upon to share this information with other parties. Being unfamiliar with the recipient and process increases tension and stress. When asked about sharing information participants do not display a similar confidence as when the information is within their domain of control. Concerning any new situation which is unfamiliar, P4 stated:

> *"But something new, I don't know how to handle it or the polices and controls around it, then maybe I would panic…"*

The severity of any data breach originating in the area where these participants work is extremely high. While participants take on the responsibility to secure information there is a growing concern about data breaches. P12 stated:

> *"We deal with data, the value of data, we know what happens if a data breach happens. So here it's me who really understands what happens if we have a data breech. It's my responsibility to make sure that the organisation has proper standards and ensure execution to make sure the data is secure."*

Most participants had an opinion on how information security should be managed, because while policies are in place, there is no clear guidance on how to execute this, which leads to frustration. Participants value security and want to do the right thing but perceived a lack of clear guidance, standards, and tools as P6 explained:

> *"In terms of actually securing data they haven't specifically given us tools to do so. We just have the industry [specific technology] security and stuff like that … they have never come to me and said you need to encrypt every single ID number. They have never done anything like that…"*

Employees are constantly faced with messages to be safe online and be vigilant about potential cyber-attacks. Participants noted how this leads to increased anxiety and a sense of resignation. Participants expressed feelings of panic, fear of getting into trouble, and fear of being hacked when faced with complex security requirements. The demographic of participants who displayed a high degree of stress are those that are older or experienced security incidents. This led to participants expressing frustration at the organisation. For example, P11 believed the organisation should deal with security related issues and stated:

> *"So, I try my best to keep myself secured but I don't feel like I should be the one to make it secure. I feel that the system or the application should have enough security built in to keep me secure. Why must I do that effort? I feel like the company that created the thing should build in security for my purpose."*

Since the appointment of the CISO the organisation has radically increased security awareness drives. The awareness activities are designed to improve security consciousness across the organisation. Participants highlighted several issues with ineffective security awareness activities, as well as the adoption of new technologies.

Participants claimed to be overwhelmed with the frequency and duration of awareness activities. For example, P9 believed there were too many phishing exercises trying to catch out employees. The time to complete awareness activities could take up to six hours every month, which involved completing online courses and questionnaires. The organisation has been quite unforgiving when it comes to completing these courses, with P7 explaining that access would be removed if employees had not completed security awareness assessments by a stated date. In an environment driven by deadlines this becomes an overload on the employee.

The effectiveness of these activities were questioned by several participants. For example, P11 stated that the activities failed to communicate details on material changes to effectively ease security concerns and

> *"… it doesn't make you want to be more secure … they [IT] just say you need to do this, and the onus is on you only, they just put all the load on the user."*

From the perspective of P12 all the activities were grounded in theory but do not offer any substantial guidance to execute on them. The consensus was that awareness activities were often no more than an academic exercise, with P3 summarising:

> *"Yes, we have all the IT security modules but are we just ticking boxes?"*

When questioned about new technologies used for data management, and specifically cloud-based technologies, participants perceived security risks. P11 voiced reservations and questioned how secure it would be:

> *"I would be very worried because I don't know how secure that is and how easy that would be for someone to hack."*

Participants welcomed and accepted the use of cloud-based technologies, provided the information stored is not sensitive. Regarding sensitive information all participants expressed concerns. Based on their experience participants foresee potential risks they are exposed to in the cloud. P2 worried about placing information in the cloud:

> *"I worry who is going to be able to access it. What is their intent ... at the end of the day I am not able to control that information."*

The perceived risks and lack of control inherent in cloud computing is a concern among the participants. However, P12 believed that conducting adequate risk assessments would be vital for storing information in the cloud.

4.2. Behavioural Adjustments

All participants displayed a high commitment to complying with security protocols. While the task of managing information should be routine to the participants, the increased security consciousness in the organisation has left participants fearful and unsure whether security processes are sufficiently followed. This led to the data specialists often creating security awareness amongst themselves, as P2 explained:

> *"... we try to enforce and create awareness in our team because we are the ones sitting with most of the data in the organisation."*

As custodians of information, they are fully aware of the need for compliance, but when security related tasks become burdensome and a barrier to their productivity, participants will forego compliance in favour of progressing efforts to achieve goals. For example, P1 admitted to making use of another employee's account to gain access to systems. The security process to get access in the organisation is not efficient, requiring layers of paperwork and approvals. P3 explained that tasks are often abandoned after attempting to log into a system:

> *"… because it is such a mission to go and email them [IT] and wait for it."*

Compliance effort is the energy spent in fulfilling security requirements. This is associated with a cost-benefit analysis, where employees will weigh up the benefits of complying versus the costs of non-compliance. While access can be circumvented, or in some cases abandoned, the sharing of sensitive information via email is a decision taken regardless of the punitive measures the employee is likely to face if there is a data breach. P2 explained:

> *"We still had reports with ID numbers … emailing data is part of the norm, however password protecting it is something that we changed."*

Participants are aware of information security compliance regulation and agreed knowing the POPIA regulation to some degree. However, they often choose to share unsecured sensitive information to ensure business continuity.

4.3. Indicators of Security Fatigue

It was noted that the organisation implements multiple layers of security. Employees must navigate physical security measures, systems with multi-factor authentication, and other security measures. When questioned about password creation and management participants revealed a few mechanisms employed to reduce cognitive demand. This includes repeating passwords, keeping password creation to the minimum system requirement, and keeping a written copy of passwords. For example, P5 used the minimum system requirements to create passwords, with the rationale that the administrators believe this is as stringent as they require the password to be to access the system. P11 provided insight into the rationale as to why keeping simple password algorithms work:

> *"Having a login profile and a password for so many devices and applications is very painful and to remember all of them is a nightmare … that's why I keep it simple, and I do remember."*

When questioned about the use of biometrics all participants agreed it would be a welcome and safer alternative, despite representing yet another layer of technical security to adopt.

The IT security division in the organisation applies strict user access protocols which can be cumbersome to navigate. Failing a security check sometimes led to the abandonment of tasks, as P3 illustrated:

> *"I put in my details, well the password, incorrect firstly. Then I tried to reset it and it said to contact the system administrator or something like that. And that was at the first try. It wasn't like we give you a temp password or whatever."*

Thus, a general sense of resigned frustration could be perceived. However, employees nevertheless seem to take responsibility for security. While P11 expressed frustration, there is an understanding that the process is in place to mitigate risk:

> *"I locked myself out of my machine and I couldn't get in ...I will sort it out because it will bother me."*

5. Discussion

The findings illustrate the complexity and nuances organisations need to manage when dealing with security and risk. While the implementation of security controls and awareness initiatives are standard practice, our findings illustrate how this affects employee perceptions, and in some cases alters behaviour in unintended ways. We believe the findings make both theoretical and practical contributions.

From a theoretical perspective the findings confirm the applicability of RHT in the security domain. This research illustrates specific examples of the homeostatic mechanism proposed by RHT, in the context of data specialists. A finding with potential for further investigation is how unfamiliarity with a process (sharing sensitive data in this context) increases tension and perceptions of risk. Furthermore, the findings also illustrate how increased security creates security fatigue, and how this could further impact risk. This presents opportunities for further investigation and incorporating the security fatigue construct into RHT. While these findings are in the context of a particular case, it can be argued that there are broader implications to similar contexts outside of this case (Yin, 2018).

From a practical perspective several observations with relevance to organisations can be made. Compliance is a choice and organisational security goals are secondary when employees' primary focus is their delivery of tasks and responsibilities (e.g., Beautement *et al.*, 2008). This has also been pointed out in the context of RHT where *"risk taking must be considered as part of a more general utility-maximizing process"* (Janssen and Tenkink, 1988, p. 429). Employees may become overwhelmed with security requirements and are often not allowed to assimilate these highly complex processes into their frame of reference and work routines (D'Arcy and Teh, 2019). In the participant group of data specialists, who have the responsibility to manage information assets in the organisation, the effort required to comply with security requirements can become unmanageable. Participants are driven by need and will forego tasks impeding their work. The findings show the importance of the organisation providing clear guidance and tools in the context of security. This will emphasise how the organisation is managing risk and help encourage desired security behaviour.

Organisations should also be cautious of using security awareness initiatives to manage risk. Previous research has shown that campaigns need to be carefully designed, to not become time consuming and confusing to participants (Scrimgeour and Ophoff, 2019). This may rapidly lead to security fatigue and seem like no more than a 'ticking boxes' exercise to employees. The findings illustrate how awareness activities demand considerable effort, which left participants despondent and with no desire to comply. In addition, the adoption of new technologies challenge employees to wilfully increase their level of knowledge to avert security incidents. In the case organisation participants took the initiative to create awareness amongst themselves, seemingly due to a heightened sense of responsibility and commitment to security, but this cannot be expected from employees in general.

The introduction of new technologies (specifically cloud-based technologies in the case organisation) should be carefully managed. The participants perceived several potential risks, which according to RHT may lead them to adjust their actions to be more secure. However, the concern may also lead to further security fatigue and a negative impact on employees. Employees are likely to feel fatigued when faced with unfamiliar tasks or the use of new technologies, regardless of the years of IT experience they had. When employees do not have adequate knowledge of security mechanisms this increases cognitive demand and stress rises. Therefore, an adequate level of knowledge may be a factor in security fatigue.

Security fatigue can be experienced along a spectrum from mild to severe with many contributing factors. Two indicators of fatigue were identified in the analysis: 1) using simplified mechanisms to manage authentication (passwords); and 2) an increase in the abandonment of tasks due to security processes. Weak password practices are an unintended consequence and presents a new risk that the organisation will need to manage. The current trend of 'passwordless' authentication (such as biometrics mentioned by participants) presents a potential solution in this case. It may also be possible to increase monitoring for abandoned tasks within information systems.

The participants, while exposed to many similar security-related tasks, often responded uniquely to security events. Interviewees showed low levels of risk tolerance and while fatigue and risk tolerance have not been empirically shown to have a causal relationship, Furnell and Thomson (2009) propose that risk tolerance will decline as fatigue increases. This could be especially important in roles where high levels of risk are present. Thus, increasing support from the organisation may be required to support employees (e.g., creating a security culture). Such support initiatives need not be technical (e.g., Alshaikh, 2020).

6. Conclusion

Employees evidence numerous risk perceptions and adjust behaviour according to RHT. They may also experience higher levels of frustration and security fatigue as demands are placed on them to maintain secure environments and to guard against security breaches. Understanding such phenomena provide important insight into the context within which employees operate, providing opportunities to improve human-centred security. This research examined risk homeostasis and security fatigue, providing several examples of how these concepts present themselves in practice. Security compliant behaviour is a multi-faceted and complex construct, and this research shows the complexity that arises from risk perceptions and linked adjustments in behaviour. This is especially true for roles that deal with sensitive information and a low tolerance for risk. While security fatigue is not readily recognisable, this study identified several indicators of the phenomena and highlights the need to understand the role security fatigue plays in security compliance and in harmonising risk.

The research focused on a very specific population and not all participants showed acute signs of security fatigue. This can be seen as a possible limitation but also an opportunity for further research. This research focused on the experience of data specialists within a specific organisation, but it is likely that their experiences are mirrored in other roles and organisations.

References

Alohali, M., Clarke, N., Li, F. and Furnell, S. (2018) ‘Identifying and predicting the factors affecting end-users’ risk-taking behavior’, Information & Computer Security, 26(3), pp. 306–326. Available at: https://doi.org/10.1108/ICS-03-2018-0037.

Alshaikh, M. (2020) ‘Developing cybersecurity culture to influence employee behavior: A practice perspective’, Computers & Security, 98, Article 102003. Available at: https://doi.org/10.1016/j.cose.2020.102003.

Beautement, A., Sasse, M.A. and Wonham, M. (2008) ‘The compliance budget: managing security behaviour in organisations’, in Proceedings of the 2008 New Security Paradigms Workshop. New York, NY, USA: Association for Computing Machinery (NSPW ’08), pp. 47–58. Available at: https://doi.org/10.1145/1595676.1595684.

Bhana, A. and Ophoff, J. (2022) ‘Security Fatigue: A Case Study of Data Specialists’, in N. Clarke and S. Furnell (eds) Human Aspects of Information Security and Assurance. Cham: Springer International Publishing (IFIP Advances in Information and Communication Technology), pp. 275–284. Available at: https://doi.org/10.1007/978-3-031-12172-2_22.

Braun, V. and Clarke, V. (2006) ‘Using thematic analysis in psychology’, Qualitative Research in Psychology, 3(2), pp. 77–101. Available at: https://doi.org/10.1191/1478088706qp063oa.

Bruemmer, M. (2016) Dispelling the Dangerous Myth of Data Breach Fatigue, Security Magazine. Available at: https://www.securitymagazine.com/articles/87014-dispelling-the-dangerous-myth-of-data-breach-fatigue.

Chen, D. and Zhao, H. (2012) ‘Data Security and Privacy Protection Issues in Cloud Computing’, in 2012 International Conference on Computer Science and Electronics Engineering. 2012 International Conference on Computer Science and Electronics Engineering, pp. 647–651. Available at: https://doi.org/10.1109/ICCSEE.2012.193.

Choi, H., Park, J. and Jung, Y. (2018) ‘The role of privacy fatigue in online privacy behavior’, Computers in Human Behavior, 81, pp. 42–51. Available at: https://doi.org/10.1016/j.chb.2017.12.001.

D’Arcy, J., Herath, T. and Shoss, M.K. (2014) ‘Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective’, Journal of Management Information Systems, 31(2), pp. 285–318. Available at: https://doi.org/10.2753/MIS0742-1222310210.

D’Arcy, J. and Teh, P.-L. (2019) ‘Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization’, Information & Management, 56(7), Article 103151. Available at: https://doi.org/10.1016/j.im.2019.02.006.

Furnell, S. (2019) ‘Security Fatigue’, in S. Jajodia, P. Samarati, and M. Yung (eds) Encyclopedia of Cryptography, Security and Privacy. Berlin, Heidelberg: Springer, pp. 1–5. Available at: https://doi.org/10.1007/978-3-642-27739-9_1591-1.

Furnell, S. and Thomson, K.-L. (2009) ‘Recognising and addressing “security fatigue”’, Computer Fraud & Security, 2009(11), pp. 7–11. Available at: https://doi.org/10.1016/S1361-3723(09)70139-3.

Hatashima, T., Nagai, K., Kishi, A., Uekusa, H., Tanimoto, S., Kanai, A., Fuji, H. and Ohkubo, K. (2018) ‘Evaluation of the Effectiveness of Risk Assessment and Security Fatigue Visualization Model for Internal E-Crime’, in 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), pp. 707–712. Available at: https://doi.org/10.1109/COMPSAC.2018.10323.

Janssen, W. and Tenkink, E. (1988) ‘Risk homeostasis theory and its critics: time for an agreement’, Ergonomics, 31(4), pp. 429–433. Available at: https://doi.org/10.1080/00140138808966689.

Jardine, E. (2020) ‘The Case against Commercial Antivirus Software: Risk Homeostasis and Information Problems in Cybersecurity’, Risk Analysis, 40(8), pp. 1571–1588. Available at: https://doi.org/10.1111/risa.13534.

Johnston, A.C., Warkentin, M. and Siponen, M. (2015) ‘An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric’, MIS Quarterly, 39(1), pp. 113–134. Available at: https://doi.org/10.25300/MISQ/2015/39.1.06.

Kearney, W.D. and Kruger, H.A. (2016) ‘Theorising on risk homeostasis in the context of information security behaviour’, Information & Computer Security, 24(5), pp. 496–513. Available at: https://doi.org/10.1108/ICS-04-2016-0029.

NIST (no date) Computer Security Resource Center. Available at: https://csrc.nist.gov/glossary/term/risk.

Ophoff, J. and Renaud, K. (2021) ‘Revealing the Cyber Security Non-Compliance “Attribution Gulf”’, in Proceedings of the 54th Hawaii International Conference on System Sciences, p. 4557. Available at: https://doi.org/10.24251/HICSS.2021.552.

Oto, B. (2012) ‘When Thinking is Hard: Managing Decision Fatigue’, EMS World, 41(5), pp. 46–50. Available at: https://pubmed.ncbi.nlm.nih.gov/22670402/.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010) Human Factors and Information Security: Individual, Culture and Security Environment. Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence Div. Available at: https://apps.dtic.mil/sti/citations/ADA535944.

Pattinson, M. and Anderson, G. (2004) 'Risk homeostasis as a factor of information security', in Proceedings of the 2nd Australian Information Security Management Conference, Securing the Future. Perth, Australia. Available at: https://www.researchgate.net/publication/221148262_Risk_Homeostasis_as_a_Factor_of_Information_Security.

Pham, H.C., Brennan, L. and Furnell, S. (2019) 'Information security burnout: Identification of sources and mitigating factors from security demands and resources', Journal of Information Security and Applications, 46, pp. 96–107. Available at: https://doi.org/10.1016/j.jisa.2019.03.012.

Renaud, K. and Warkentin, M. (2017) 'Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact', in Proceedings of the 2017 New Security Paradigms Workshop. New York, NY, USA: Association for Computing Machinery (NSPW 2017), pp. 57–69. Available at: https://doi.org/10.1145/3171533.3171534.

Sasse, A. (2015) 'Scaring and Bullying People into Security Won't Work', IEEE Security Privacy, 13(3), pp. 80–83. Available at: https://doi.org/10.1109/MSP.2015.65.

Scrimgeour, J.-M. and Ophoff, J. (2019) 'Lessons Learned from an Organizational Information Security Awareness Campaign', in L. Drevin and M. Theocharidou (eds) Information Security Education. Education in Proactive Information Security. Cham: Springer International Publishing (IFIP Advances in Information and Communication Technology), pp. 129–142. Available at: https://doi.org/10.1007/978-3-030-23451-5_10.

Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S. (2016) 'Security Fatigue', IT Professional, 18(5), pp. 26–32. Available at: https://doi.org/10.1109/MITP.2016.84.

Taylor, S., Bogdan, R. and DeVault, M. (2016) Introduction to Qualitative Research Methods: A Guidebook and Resource. 4th edition. Hoboken, New Jersey: John Wiley & Sons.

Warkentin, M., Goel, S., Williams, K.J. and Renaud, K. (2018) 'Are we Predisposed to Behave Securely? Influence of Risk Disposition on Individual Security Behaviours', European Conference on Information Systems (ECIS) Research-in-Progress Papers. Available at: https://aisel.aisnet.org/ecis2018_rip/25.

Wilde, G.J.S. (1982) ‘The Theory of Risk Homeostasis: Implications for Safety and Health’, Risk Analysis, 2(4), pp. 209–225. Available at: https://doi.org/10.1111/j.1539-6924.1982.tb01384.x.

Wilde, G.J.S. (1998) ‘Risk homeostasis theory: an overview’, Injury Prevention, 4(2), pp. 89–91. Available at: https://doi.org/10.1136/ip.4.2.89.

Yin, R. (2018) Case Study Research and Applications: Design and Methods. 6th edition. Los Angeles: SAGE Publications, Inc.

Appendix A

Table II. Interview questions

A. Participant information
1. Please state your gender. 2. Please state your age. 3. What is your job role in the organisation and how long have you worked in this role?
B. Security-related perceptions and behaviours
1. How comfortable are you generally with sharing and having access to sensitive information? 2. How often do you use public access Wi-Fi? 3. Are you comfortable downloading software or content from any sites? Do you think about the potential risks you are facing? 4. To secure access to multiple devices and application, we often make use of passwords. How do you manage your passwords to make sure you can access what you need when you need it? 5. If you had a choice, would you choose to use biometrics to access your devices and applications as opposed to password control? 6. What is your view on security awareness programs conducted in the organisation? 7. If there is a cyber-attack in your organisation, do you believe you would need to re-evaluate how you perform your tasks? How would you adjust your behaviours? 8. Many organisations are strategically implementing cloud solutions. What do you think about cloud security, and would you be comfortable to have your personal information stored in the cloud?
C. Risk and responsibility
1. Would you describe yourself as risk averse or a risk-taker? Can you give me an example to illustrate your choice? 2. As someone who works with data what is your view on the increased hyper vigilance around data security? 3. How familiar are you with data privacy laws like POPIA and GDPR? 4. Has the organisation clearly outlined to you, as an employee who handles data daily, the policies and procedures in place to protect data from vulnerabilities? 5. Do you feel confident the organisation has empowered you as a data specialist to deal with any potential data breaches resulting from your daily activities? 6. Do you believe you share in the responsibility to manage and maintain data security? Why? 7. Do you believe the organisation is at risk of cyber-attacks? Why do you think that? 8. Do you believe you have a part to play in maintaining organisational security?
D. Security fatigue
1. Have you ever abandon doing a task due to security restrictions? 2. Please describe an instance where organisational security was a barrier to you doing your job. What steps did you take to overcome these barriers?