

A qualitative case study of cybersecurity fatigue and human-centric vulnerabilities in the SaaS sector

Cassidy Norton and Zainab Ruhwanya 

*Department of Information Systems, University of Cape Town,
Cape Town, South Africa, and*

Jacques Ophoff 

*Department of Information Systems, University of Cape Town, Cape Town,
South Africa, and Department of Cybersecurity and Computing,
Abertay University, Dundee, UK*

Received 2 February 2026
Revised 13 August 2026
Accepted 17 September 2026

Abstract

Purpose – Cybersecurity fatigue is an important organisational issue, especially in high-pressure operational contexts such as Software-as-a-Service environments. As organisations implement stricter security controls and mandatory training, this can inadvertently place psychological strain on employees. This study/paper aims to identify specific operational demands and workflow characteristics contributing to employee cybersecurity fatigue and analyse the subsequent behavioural implications.

Design/methodology/approach – This study adopted an interpretivist, qualitative approach, using semi-structured interviews with employees from various departments to explore the causes and behavioural impacts of cybersecurity fatigue. A single organisation was used as case study.

Findings – The findings identified several key contributors: workflow disruption, cybersecurity decision overload, work overload and poor understanding of risk. These were associated with secondary elements such as repetitive access requests, security checks overload, a lack of real-world examples and generic training. The study also examined how these factors impact employee behaviour, revealing that fatigue often leads to disengagement, neglect of protocol and abandonment of cybersecurity tasks, especially training.

Originality/value – Attitudinal fatigue, employees' negative perceptions of cybersecurity, emerged as a critical influence on compliance and overall cyber resilience. A conceptual model is proposed by integrating the study's findings with the four-component model of cybersecurity fatigue, offering a foundation for future research. This model may be useful for examining cybersecurity fatigue and developing targeted interventions to reduce its impact. The authors recommend implementing contextualised training with real-world examples and streamlining security processes to reduce workflow disruption and frustration.

Keywords Cybersecurity, Fatigue, Human factors, Case study

Paper type Research paper



© Cassidy Norton, Zainab Ruhwanya and Jacques Ophoff. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/>

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-02-2026-0050

1. Introduction

In the current digital landscape, cybersecurity threats and data breaches have escalated significantly, prompting modern organisations to increase investments in cybersecurity systems and infrastructure (IBM, 2024). To defend sensitive assets against these threats, organisations typically deploy increasingly stringent and layered cybersecurity controls, ranging from complex multi-factor authentication (MFA) to continuous compliance monitoring and mandatory security training. While these security measures are technically sound, their cumulative effect on the workforce is often overlooked. Specifically, these requirements can inadvertently place substantial cognitive and psychological strain on employees, leading to a negative phenomenon known as cybersecurity fatigue (Furnell and Thomson, 2009).

Cybersecurity fatigue is characterised by a state of mental exhaustion, diminished attention and eventual disengagement from security practices (Cram *et al.*, 2021). Far from being a minor inconvenience, cybersecurity fatigue poses a systemic risk to organisations. When employees reach their psychological limits, they experience a breakdown in security awareness, which directly undermines the effectiveness of technical security controls and introduces significant human-centric vulnerabilities (Hull, 2017). Investigating and mitigating this issue requires a nuanced exploration of the cognitive and behavioural dynamics of employees under security strain. Despite this need, existing cybersecurity literature has historically treated the human factor as a mechanical link, providing limited qualitative insights into the cognitive, emotional and situational dimensions of cybersecurity fatigue and its real-world implications for employee behaviour (Glaspie and Karwowski, 2018; Nobles, 2022).

While prior behavioural security research has investigated the consequences of cybersecurity fatigue (e.g. Cram *et al.*, 2021; Reeves *et al.*, 2023, 2025) and proposed general models, such as the well-known four-component model of cybersecurity fatigue (Reeves *et al.*, 2021), there is little known regarding its operational manifestation in specific, highly demanding workplace environments. In particular, how cybersecurity fatigue develops and influences behaviour within highly fluid, cloud-centric Software-as-a-Service (SaaS) organisations. SaaS environments present a high-pressure operational context:

- They operate under a continuous, real-time access paradigm where providers bear direct responsibility for safeguarding large volumes of sensitive client data (Rath *et al.*, 2019).
- Their employees must navigate a complex, highly integrated Web of SaaS platforms and third-party tools, which requires constant, repetitive verification (Humayun *et al.*, 2022).
- They are characterised by fast-paced environments, where workflow disruptions can directly impede core job performance, creating a tension between operational productivity and security compliance. Such conditions may increase employees' propensity to bypass security policies to complete tasks, while time pressure reduces security-compliant behaviour (Gerdenitsch *et al.*, 2023; Jiang and Zhang, 2023).

Consequently, general models of cybersecurity fatigue fail to capture the specific operational triggers and behavioural coping mechanisms that occur in the SaaS sector. This study addresses this research gap by providing an in-depth qualitative examination of how cybersecurity fatigue is triggered, processed and manifested behaviourally within a SaaS provider. It focuses on the intersection of operational SaaS workflows and employee behavioural compliance, posing the following research questions:

- RQ1. What specific operational demands and workflow characteristics contribute to cybersecurity fatigue among employees within a SaaS organisational environment?

RQ2. How does cybersecurity fatigue manifest in observable, non-compliant workplace behaviours and what are the specific implications of these behaviours for organisational security?

This paper is an extended version of research originally presented at the 19th IFIP WG 11.12 International Symposium on Human Aspects of Information Security and Assurance (HAISA 2025) (Norton *et al.*, 2026). This journal version expands upon the original paper by strengthening the theoretical foundation, providing a more detailed account of the research design and presenting an enriched qualitative analysis incorporating newly analysed empirical data and participant quotes. The findings provide dual contributions in the topic area:

- (1) Theoretical contributions: We advance behavioural theory by contextualising the four-component model (Reeves *et al.*, 2021) within a SaaS environment. We provide empirical evidence showing how specific factors like workflow disruption and cybersecurity decision overload translate directly into three discrete behavioural outcomes: abandonment of cybersecurity tasks, neglect of proper protocol and disengagement from training. We also contribute to theoretical boundaries by discussing the absence of advice-related fatigue in this operational context.
- (2) Practical contributions: We offer actionable, evidence-based recommendations for SaaS managers and CISOs. Rather than recommending simple increases in training volume, we outline concrete strategies for contextualising training with role-specific, real-world examples and streamlining security processes (such as automating access ticketing systems) to reduce daily frustration, mitigate cognitive overload and ultimately foster a resilient security culture.

The remainder of this paper is organised to systematically address the research questions. Section 2 reviews existing human factors in cybersecurity and establishes Reeves *et al.*'s (2021) four-component model of cybersecurity fatigue as the theoretical foundation. Section 3 details our interpretivist qualitative case study methodology, the purposive sampling strategy within the SaaS sector and the thematic analysis approach used to analyse our interview data. Section 4 presents our empirical analysis and findings, illustrating how work-flow disruption, decision overload, work overload and poor understanding of risk manifest in the daily experiences of SaaS employees. Section 5 maps these empirical findings to our proposed conceptual model, discusses the pathways of employee fatigue and details strategic security recommendations for organisations. Finally, Section 6 summarises our key findings and outlines opportunities for future research.

2. Literature review and theoretical framework

To understand the complex interplay between organisational security demands and individual employee behaviour, this study examines how cybersecurity fatigue manifests as a psychological and operational risk. Rather than viewing compliance failures as isolated acts of employee negligence, contemporary human factors research increasingly conceptualises non-compliance as a systemic out-come of cognitive, emotional and physical exhaustion (Glaspie and Karwowski, 2018; Pham *et al.*, 2019; Nobles, 2022). This literature review establishes the theoretical foundation of our study by introducing the four-component model of cybersecurity fatigue (Reeves *et al.*, 2021) and organising the underlying literature around the task-level, organisational and educational antecedents that drive fatigue-induced behaviours.

2.1 Theoretical foundation: the four-component model

Over the years, numerous technical solutions have been developed to address cybersecurity vulnerabilities within organisations. However, while these solutions can mitigate certain risks, they are insufficient for preventing all security incidents. Increasingly, research suggests that the effectiveness of cybersecurity relies as much, if not more, on human behaviour (Hughes-Lartey *et al.*, 2021; Moustafa *et al.*, 2021).

As security demands become more complex, employees experience negative psychological effects, giving rise to a phenomenon known as cybersecurity fatigue. This term has been defined in various ways. Early recognition of the phenomenon conceptualised it in terms of effort and difficulty of security requirements and priorities of the individual and organisation (Furnell and Thomson, 2009). It generally refers to a state of mental exhaustion or disengagement from security practices, often resulting in employees neglecting or bypassing security protocols (Stanton *et al.*, 2016). More specifically, cybersecurity fatigue is described as a form of work-related disengagement that pertains uniquely to security responsibilities (Reeves *et al.*, 2021). This issue poses a growing threat to organisations, given that employees are frequently regarded as the most vulnerable point in the security chain (Acuña, 2016; Johnston *et al.*, 2019; Hughes-Lartey *et al.*, 2021).

While previous studies have highlighted the stressful nature of security compliance (D'Arcy *et al.*, 2014; Ament and Haag, 2016) the four-component model of cybersecurity fatigue proposed by Reeves *et al.* (2021) provides the first comprehensive framework to categorise the diverse dimensions of security-related exhaustion. The model is structured along two primary dimensions: the sources of fatigue (action vs advice) and the types of fatigue (cognitive vs attitudinal).

2.1.1 Sources of fatigue: action versus advice. Action-related fatigue arises when employees are continually required to perform tasks or make decisions to secure their organisational environment. The cumulative burden of continuous MFA requests, password updates and data-handling permissions generates high friction, leading to frustration, mental weariness and eventual fatigue (Pham *et al.*, 2019; Cram *et al.*, 2021; Robinson, 2023; Hsu *et al.*, 2024). Studies report that such pressures have contributed to elevated stress levels and mental health concerns (ISACA, 2020; Sheridan, 2020). Despite being a widespread issue, limited research has examined how action fatigue interacts with technical cybersecurity solutions (Dykstra and Paul, 2018). When security-related responsibilities become overwhelming, employees may deprioritise compliance in favour of completing their primary job functions, increasing the risk of breaches (Bhana and Ophoff, 2023).

In contrast, advice-related fatigue stems from excessive, inconsistent or overly complex security guidance. While cybersecurity awareness initiatives can improve compliance, when organisations inundate employees with frequent, dense or conflicting instructions the resulting ambiguity diminishes employees' sense of agency, inducing anxiety and disengagement (Ogawa *et al.*, 2020; Bhana and Ophoff, 2023). When advice is unclear or contradictory, it diminishes employees' sense of control and increases the likelihood of poor security behaviours (Reeves *et al.*, 2021). Even well-intentioned awareness campaigns can contribute to fatigue if not well-coordinated and clearly communicated (D'Arcy *et al.*, 2014; Davis *et al.*, 2023).

2.1.2 Types of fatigue: cognitive versus attitudinal. With cognitive resources being finite, there is a limit to how much information employees can absorb and retain. Cognitive fatigue occurs when employees are overwhelmed by the volume of security-related information they are expected to process (Robinson, 2023). In many organisations, the complexity and length of security policies contribute significantly to cognitive overload. Employees frequently report difficulty processing dense or excessive content, resulting in disengagement (Cram *et al.*, 2021). Under cognitive fatigue, individuals struggle to process security-critical information, rendering

them more vulnerable to social engineering and prone to overlooking critical security warnings (Montañez *et al.*, 2020; Reeves *et al.*, 2021).

Attitudinal fatigue represents a deeper, more permanent shift in an employee's emotional and psychological stance towards security (Reeves *et al.*, 2021). If employees view security protocols as burdensome or unnecessary, they are more likely to become disengaged and non-compliant (Alotaibi *et al.*, 2016; Robinson, 2023). A negative outlook can breed resentment and apathy, leading to resistance against established procedures and greater exposure to risk (Rocha Flores *et al.*, 2014; Davis *et al.*, 2023). Employees suffering from attitudinal fatigue may come to regard security measures as pointless, further exacerbating non-compliance (Reeves *et al.*, 2021).

In this study, the four-component model serves as the direct theoretical lens for our qualitative inquiry. It informs the thematic structure of the interview guide (see Table 1) and provides the analytical categories for our thematic coding, enabling us to trace how real-world SaaS operational pressures map onto specific forms of employee exhaustion.

2.2 Task-level antecedents: workflow disruption and compliance overload

Organisational security measures are often designed under the assumption of perfect compliance, ignoring the operational environments in which employees operate. When security controls are

Table 1. Interview guide

Category	Questions
Introduction	Can you state your age? How long have you been at the organisation?
Action-related	Do you feel compliance with cybersecurity regulations is reasonable for your work role? How do you feel about the actions you are required to take to comply with cybersecurity regulations? Do you feel the actions you are required to take influence you in your job role? (negatively or positively). Can you give an example? Do you feel the actions you are required to take influence your regular job responsibilities? If so, how? Have you ever abandoned doing a task due to cybersecurity? Can you give an example?
Advice-related	Do you feel the information shared by the company using training and documented regulations surrounding cybersecurity is clear and easy to understand? Do you think there is too little or too much information? How do you feel about the advice you receive from the company about cybersecurity?
Cognitive	Are you required to participate in large amounts of cybersecurity training? If so, how does this affect you and your behaviour? Can you give an example? Are there large amounts of regulations you are required to understand? If so, how does this affect you and your behaviour? Can you give an example?
Attitudinal	What is your attitude towards cybersecurity as a whole? Considering all the factors we have discussed above, has your attitude towards cybersecurity changed over time? If so, how?
Other	Do you have anything else you would like to share about how you feel about cybersecurity and cybersecurity fatigue?

Source(s): Authors' own work

overly intrusive, they disrupt natural work-flows and generate significant compliance friction (Herley, 2009; Stanton *et al.*, 2016).

2.2.1 Friction in access controls and workflow delays. Modern security frameworks, such as zero-trust architectures, mandate continuous verification through repetitive access requests and rigid authorisation protocols. While technically sound, these measures introduce operational delays that slow business workflows. When compliance is perceived as excessive or unmanageable, employees are more likely to prioritise routine work tasks over security obligations – the resulting friction acts as a major driver of action-related and attitudinal fatigue (Bhana and Ophoff, 2023). This disruption creates a psychological trade-off, forcing employees to choose between strict security adherence and timely task execution (Stanton *et al.*, 2016).

2.2.2 Interruption and desensitisation. Continuous security interruptions, such as frequent MFA prompts, degrade employee focus and break cognitive flow. This may lead to sensory and behavioural desensitisation, whereby employees become less attentive to security threats and the behaviours intended to mitigate them (De Vos *et al.*, 2017; Johnston *et al.*, 2019). Over time, employees suffer from “habituation” where security alerts and authentication checks are processed less thoughtfully (Vance *et al.*, 2018).

2.3 Organisational antecedents: workplace pressure and work overload

An employee’s cognitive and emotional capacity is not dedicated solely to security compliance but must be shared with their work obligations. Cybersecurity fatigue is therefore fundamentally compounded by broader organisational pressures and work overload.

2.3.1 Cognitive capacity and the dual-task conflict. Human cognitive resources are strictly finite. Within modern, high-pressure environments, employees experience a persistent dual-task conflict between their primary job duties (which carry clear performance incentives) and security compliance (which is often perceived as non-productive overhead) (Ament and Haag, 2016). When work-related deadlines and cognitive demands escalate, employees experience a divided attention effect. Under intense task pressure, cognitive capacity is entirely consumed by core operations, forcing employees to cognitively withdraw from security compliance to conserve mental bandwidth (Pfleeger and Caputo, 2012; Montañez *et al.*, 2020).

2.3.2 Work overload and burnout. Chronic work overload, characterised by excessive volumes of data processing, emails and meetings, depletes executive functioning and drives broader work-related burnout. When combined with rigid security compliance protocols, this dual burden can diminish work quality (Posey *et al.*, 2011) and accelerates the onset of security burnout (Pham *et al.*, 2019). This state of exhaustion results in perceived “laziness” or “workarounds”, where employees actively compromise security standards. Examples include using weak or slightly modified, passwords to reduce the mental effort required to navigate frequent system-enforced security demands (Bhana and Ophoff, 2023).

2.4 Educational antecedents: security training and risk perception

Non-compliant behaviour may arise from insufficient employee awareness of security requirements. While security education, training and awareness (SETA) programs are designed to mitigate human risk, poorly designed educational initiatives can inadvertently worsen security fatigue.

2.4.1 The cognitive cost of generic training. SETA programs are a primary tool for cultivating a security culture (Safa *et al.*, 2016). However, many organisations deploy one-size-fits-all training that is overly generic, highly repetitive and disconnected from employees’ daily operational realities. Generic training programs frequently focus on compliance checklists rather than contextualised threat scenarios. Rather than enhancing competence, repetitive

and non-relevant training imposes an unproductive cognitive load (Bhana and Ophoff, 2023). Employees quickly recognise that the training does not add value to their specific roles, prompting them to disengage (Reeves *et al.*, 2023).

2.4.2 The gap between awareness and risk understanding. During training, employees are required to devote time and cognitive effort to understanding and applying the organisation's information security measures (D'Arcy *et al.*, 2014). These measures frequently involve complex technical terminology, which can be difficult to interpret (Hsu *et al.*, 2024). Complexity may lead to confusion and increased stress (Tarafdar *et al.*, 2007), and may contribute to cybersecurity fatigue and subsequent disengagement from learning activities.

A critical gap exists between basic security awareness (i.e. knowing a rule exists) and deep risk understanding with comprehension of the practical impact of a security failure (Nurse *et al.*, 2025). Without a clear understanding of the underlying risk and practical, real-world consequences, employees perceive security measures as arbitrary, bureaucratic constraints (Bhana and Ophoff, 2023). Cultivating deep risk perception requires dynamic adaptation, real-world examples and interactive learning formats (such as simulated exercises or security workshops) that demonstrate how individual actions directly influence organisational and client information security (Hatzivasilis *et al.*, 2020).

3. Methodology

This study adopts an interpretivist research philosophy, reflecting its focus on the subjective experiences and perceptions of individuals. Aligned with a qualitative research strategy, the research is exploratory in nature, aiming to investigate cybersecurity fatigue among employees. Rather than seeking definitive conclusions, the study seeks to identify emergent ideas, patterns and themes.

3.1 Case study

The case organisation operates within the SaaS sector, a cloud computing model where service providers manage infrastructure and deliver software access via Web browsers (Palos-Sanchez *et al.*, 2017). SaaS adoption has expanded rapidly, with approximately 70% of businesses currently using such platforms, and this figure is expected to reach 85% in 2025 (Howarth, 2024). Given the critical responsibility SaaS providers have in protecting client data, understanding employee cybersecurity behaviour within these environments is essential (Arce, 2020; Rahman and Pribadi Subriadi, 2022).

3.2 Research instrument

The data collected in this study reflects individual employees' experiences and perceptions of cybersecurity fatigue and is therefore qualitative in nature. To elicit this subjective data, semi-structured interviews were used. The use of open-ended questions enabled participants to describe their experiences in their own words, while the semi-structured format allowed the interviewer to pursue emergent topics beyond the predefined research questions. This flexibility supported the identification of unanticipated themes relevant to cybersecurity fatigue.

An interview guide was used to ensure consistency across interviews. This was informed by the four-component model of cybersecurity fatigue and is described in Table 1. Each interview began with the interviewer introducing themselves, confirming that informed consent had been obtained and requesting permission to audio record the session. The interviewer then explained the purpose of the study, which was to examine the prevalence of cybersecurity fatigue within the organisation, the factors contributing to it, and its influence

on employee behaviour and attitudes towards cybersecurity. The interview then proceeded with the guided questions.

3.3 Data collection

The study used a purposive sampling strategy, which involves the deliberate selection of participants based on predefined characteristics relevant to the research objectives. Participants were selected from different departments within the case organisation to capture a range of experiences and perspectives related to cybersecurity fatigue. To protect participant anonymity, departmental affiliations are not disclosed, in accordance with employee requests.

Sampling across multiple departments was intended to enhance the diversity of experiences represented in the data, as employees within the same department may share similar cybersecurity responsibilities and regulatory requirements. Ethical approval for the study was granted by the educational institution of the researchers, prior to data collection. In addition, approval to recruit participants was obtained from the organisation’s managing director. Following this authorisation, employees were invited to participate in the study on a voluntary basis.

Data collection took place across a period of roughly ten weeks in mid-2024. The study involved eight participants selected from a range of departments to capture diverse perspectives. Participant experience at the organisation ranged from one to almost eight years, with an average of about three years. All participants held a tertiary qualification. The participants are summarised in Table 2.

3.4 Data analysis

Data analysis involves the systematic examination of collected data to identify patterns, relationships and underlying meanings relevant to the research objectives. In this study, thematic analysis was used to analyse the qualitative interview data. Thematic analysis is a widely used qualitative analytic method that focuses on identifying, analysing and reporting recurring themes within a data set (Braun and Clarke, 2006).

Thematic analysis is particularly well suited to qualitative studies that seek to explore participants’ experiences and perceptions, as it enables the researcher to capture both explicit and implicit meanings in the data (Clarke and Braun, 2017; Braun et al., 2019). Its flexibility allows it to be applied across a range of theoretical frameworks without requiring adherence to a specific epistemological stance, making it appropriate for exploratory research in applied domains such as cybersecurity. By enabling the identification of common and divergent experiences of cybersecurity fatigue, thematic analysis provides a robust framework for interpreting how organisational and individual factors influence employee attitudes and behaviours. Its

Table 2. Participant overview

Id	Time at organisation	Level of education
1	2 year 6 month	Diploma in information technology
2	7 year 6 month	BSc honours in computer science
3	2 year 6 mo	BSc in mathematics and computer science
4	1 year 6 month	BSc honours in information systems
5	1 year	BSc in mathematical science
6	3 year	BA in communication and psychology
7	1 year	BCom in information systems
8	2 year 11 month	Diploma in marketing

Source(s): Authors’ own work

transparency and structured phases of analysis also contribute to methodological rigour and trustworthiness in qualitative re-search (Nowell *et al.*, 2017). The NVivo [1] Computer-Assisted Qualitative Data Analysis Software supported the coding and organisation of themes.

4. Analysis and findings

Security fatigue is defined as a specific form of work disengagement related to cybersecurity responsibilities (Reeves *et al.*, 2021). This section presents the key themes identified in the study and their influence on cybersecurity fatigue among employees in the case organisation's cloud computing environment. The primary contributing factors include *workflow disruption*, *cybersecurity decision overload*, *work overload* and *poor understanding of risk*. These were associated with secondary elements such as *repetitive access requests*, *security checks overload*, *a lack of real-world examples* and *generic training*. The study also examined how these factors impact employee behaviour, revealing that fatigue often leads to *disengagement*, *neglect of protocol* and *abandonment of cybersecurity tasks*, especially training.

4.1 Workflow disruption

Cybersecurity practices, while essential, can significantly disrupt employee work-flows. Repetitive access requests and frequent security checks were identified as key drivers of frustration and action fatigue, which is a form of exhaustion caused by repetitive or demanding actions (Pham *et al.*, 2019; Cram *et al.*, 2021; Reeves *et al.*, 2021).

4.1.1 Repetitive access requests. Security protocols requiring formal access requests, while effective in safeguarding sensitive data, often delay workflows. An example from the case organisation is that employees must submit formal access request tickets for sensitive information, replacing the informal, immediate approval process previously handled by managers. This system was introduced to reduce the risk of data breaches by ensuring that access is carefully reviewed and approved by the appropriate team. The process requires the employee to submit a formal access request or "ticket", detailing the specific permissions needed. Once submitted, the ticket is assigned to the appropriate individual or team for review and placed in a queue. The request is then assessed and either approved or denied based on established criteria. While it enhances security by limiting access to authorised personnel, the process can take up to three days, causing delays for employees. Participants described these procedures as frustrating, particularly when approval took several days. One participant stated:

The access requests are both annoying and frustrating because they prevent me from completing tasks and finishing tickets on time. [P5]

In this context, tickets refer to routine work tasks assigned to employees. Although the system may be effective in strengthening security, it can also have unintended negative effects on employee behaviour. This finding aligns with the concept of regulation and compliance overload identified in the literature, where mandatory security requirements contribute to frustration and cybersecurity fatigue. Such fatigue can lead to disengagement and encourage employees to seek ways to bypass established regulations (Bhana and Ophoff, 2023).

The requirement to submit access requests and wait for approval, as reported by employees in this study, reflects the characteristics of action fatigue. In some cases, this fatigue prompts employees to bypass regulatory and compliance procedures in an effort to complete their work more efficiently, as illustrated by another participant:

In theory, yes, I log tickets. In practice, I tend to just bug people.

[...] I need to do this to work, fix it. [P7]

This example demonstrates how cybersecurity fatigue can lead employees to neglect established protocols. Within the proposed model, neglect of protocol is identified as a behavioural outcome of workflow disruption. Such behaviour increases organisational vulnerability to cyber-attacks and data breaches. Consistent with existing research, frequent interruptions caused by security measures can result in employee disengagement from cybersecurity practices (Glaspie and Karwowski, 2018), thereby heightening the organisation's overall security risk.

4.1.2 Security checks overload. In addition to submitting access requests, employees must complete various security checks during their workday, such as two-factor authentication (2FA).

While these measures are essential for safeguarding sensitive information, they can disrupt workflow, contribute to frustration and ultimately lead to fatigue. Participants explained how:

The constant requirement to complete these security checks interrupts my focus and makes it harder to stay productive. [P4]

Sometimes we want to go onto the HR platform, and I have to do the whole 2FA. I'm like, stuff this, I do not need this information. [P7]

These disruptions contribute to cognitive fatigue, which occurs when employees reach the limits of their mental capacity to engage with security tasks (Reeves *et al.*, 2021; Cram *et al.*, 2021). This cognitive strain can lead to disengagement and decreased vigilance. Cognitive fatigue has been identified as a significant contributor to overall cybersecurity fatigue (Pham *et al.*, 2019; Bhana and Ophoff, 2023). Similar to repetitive access requests, this links to regulation and compliance overload. An excessive number of security checks can not only intensify fatigue but also overwhelm employees, leading them to abandon tasks entirely. As a result, employees may begin to perceive cybersecurity requirements as obstacles to productivity rather than as protective measures.

4.2 Cybersecurity decision overload

Another source of fatigue stems from the burden of making constant security-related decisions. Some employees expressed anxiety and uncertainty, particularly around the fear of making a critical mistake:

The constant decision-making is intimidating, and anxiety driven. [P5, a junior employee]

Research shows that increasing the number of options, and having limited time, make decisions more difficult and frustrating (Haynes, 2009). This phenomenon has received little attention in security research, but is closely associated with uncertainty. Employees may be unsure about regulations they are expected to follow, which can contribute to increased stress and anxiety. This uncertainty is intensified by the awareness that mistakes can have serious consequences. Such conditions can lead to decision paralysis, where anxiety and hesitation result in poor or suboptimal decision-making (Yang *et al.*, 2015). Consequently, employees may make incorrect security-related decisions, potentially exposing the organisation to an increased risk of cyber-attacks.

This pressure can result in minimal compliance. For example:

My passwords are definitely becoming less secure. I'm becoming lazy.

[...] If I've got to change a password every 30 days, I'm not going to think up a new one. Add an exclamation, change that exclamation point to a hash [...] If you come up with a secure password and memorise it, by the time you've memorised the thing, you must change the thing again. So, what's the point? [P7].

Such behaviour reflects attitudinal and action fatigue. When employees start to perceive security-related tasks, such as regularly updating passwords, as inconvenient or onerous, they

may become less motivated to fully comply. Employees may do the bare minimum, for example by making only minor changes to an existing password, increasing the likelihood of security vulnerabilities and potential cyber breaches.

4.3 Work overload

Work overload was another contributor to fatigue, leading to the dual-task conflict between operational productivity and security compliance (Ament and Haag, 2016). Employees reflected the need to prioritise job-related tasks over security obligations:

I have more important things to do, which is also another important factor. We don't necessarily have time to go through a two-hour long course. We've got important work to get done with deadlines, and now you're making me do a course. Where's my attention? I'm going to be worrying about work, not paying attention to the course. We get paid to work and we get in trouble if you don't get the work done. You don't get paid to do the compliance training and get into more trouble for the work than for the training. [P7]

This quote illustrates that work overload does not only affect an employee's attitude towards compliance but also drains their cognitive focus ("Where's my attention?"), making genuine engagement with security training intellectually impossible under deadline pressure. Because organisations actively reward productivity and penalise missed deadlines, employees must divide their finite cognitive resources between these competing demands. Under high-pressure deadlines, an employee's cognitive capacity is consumed by their primary work tasks, inducing cognitive fatigue and leaving little remaining mental capacity for secondary security compliance (Pfleege and Caputo, 2012; Montañez *et al.*, 2020).

This cognitive exhaustion may translate into attitudinal fatigue, where security training is resented as an obstructive, non-productive overhead. Consequently, employees abandon security training because the organisational incentives heavily favour operational output over security box-checking. This perceived work versus security trade-off increases the risk of oversight and reduces engagement with cybersecurity training and tasks (Pfleege and Caputo, 2012). The example highlights the influence of top management in shaping employee attitudes towards security. Top management should use mechanisms such as perceived legitimacy, visible commitment and fairness to foster a strong security culture and guide appropriate behaviours (Hu *et al.*, 2012).

4.4 Poor understanding of risk

A key insight from the research was the significant role that risk perception plays in employee engagement with cybersecurity. Without a clear understanding of the implications, employees are less likely to comply with protocols:

In my experience, they [employees] are aware. However, it is generally a lack of understanding of the underlying risk that prevents action. [P1]

Research indicates that employees often show little concern about cyber-attacks or how to respond to them until they have personally experienced such an incident (Sun and Lee, 2016). This limited awareness is largely shaped by generic cybersecurity training and a lack of real-world examples that illustrate actual risks.

4.4.1 Lack of real-world examples. In the absence of concrete, sector-specific examples demonstrating how a single error can compromise sensitive data, employees may perceive security controls as arbitrary administrative barriers rather than essential safeguards for organisational and client security (Bhana and Ophoff, 2023; Nurse *et al.*, 2025). Participants stressed the value of contextualising cybersecurity risks:

Real-world examples of what could happen or what the risks are definitely play a bigger role in my caution. [P4]

If you show people how a breach could directly affect their role, they'd take it more seriously. [P8]

The incorporation of real-world examples enables employees to better appreciate the consequences of their actions and, in turn, encourages more meaningful engagement with organisational cybersecurity practices. However, example empirical data on cyber risks remains limited (Cremer *et al.*, 2022). This is partly because many organisations that experience cyber incidents choose not to publicly disclose them (Eling and Schnell, 2016; Thomas, 2018). As a result, areas such as cybersecurity risk management are constrained by this lack of available data.

Despite these limitations, existing literature suggests that integrating real-world examples into cybersecurity training can significantly enhance organisational protection against cyber-attacks. Simulations and scenario-based exercises grounded in real incidents provide employees with practical, hands-on experience, which improves their understanding of cybersecurity risks and responses (Hatzivasilis *et al.*, 2020). In contrast, the absence of such examples not only reduces employees' comprehension of cybersecurity risks but also weakens their awareness of the potential consequences of non-compliant or insecure behaviour.

4.4.2 Generic training. During the interviews, participants consistently reported that the cybersecurity training they receive is overly generic, which leads to disengagement with the material. Rather than providing meaningful, role-specific guidance, this training focuses on repetitive "common-sense" topics. A lack of context and explanation behind the training requirements were highlighted:

[...] it doesn't really go into specifics of why we're doing things and why things are the way they are, and why you shouldn't do this and that. So I don't think it's very educational. [P7]

Much of the training focuses on topics such as identifying phishing emails — content many employees perceive as basic or already well understood, resulting in the belief that it adds little value. It appeared that employees do not perceive the training as excessive or overly complex, but rather as lacking relevance to their role:

It's mostly common sense, to be honest. I don't think it adds much value, at least not for me [...] There's nothing really specific to my role, and a lot of it is repetitive. [P8]

Because this training fails to stimulate genuine cognitive engagement or offer new insights, it imposes an unproductive cognitive load on employees, who must dedicate time and effort to processing redundant information. This leads to cognitive fatigue, as employees find the repetitive material mentally draining (Reeves *et al.*, 2023). Simultaneously, it fosters attitudinal fatigue by convincing employees that security training holds no practical value for their daily operational roles.

This perceived irrelevance contributes to low engagement, with some employees admitting to accelerating training videos simply to complete them. This was achieved by increasing playback speed or using browser extensions to speed up training content. Disinterest in training is a phenomenon existing literature links to repetition and lack of relevance (De Vos *et al.*, 2017; Johnston *et al.*, 2019) and may lead to potential negligence (Pham *et al.*, 2019). While generic training may not directly cause fatigue, it does undermine engagement, reinforcing the argument that cybersecurity training cannot adopt a one-size-fits-all approach (Reeves *et al.*, 2023).

Given the rapidly evolving nature of cybersecurity threats, disengagement with training risks creating knowledge and skill gaps that could expose organisations to cyber-attacks. Participants emphasised the need for contextualised, role-specific training supported by real-

world examples to help employees better understand both the risks and consequences of their actions, e.g.:

I'd be curious to see more advanced or specialised training [...] there are definitely gaps in the current training. [P8]

5. Discussion

The examples identified through the analysis illustrate the operational demands and workflow characteristics that contribute to cybersecurity fatigue among employees within the case study organisation. These findings address the first research question and are synthesised in a conceptual model presented in Figure 1. The model draws on elements from the four-component model by Reeves *et al.* (2021), specifically incorporating action-related fatigue, cognitive fatigue and attitudinal fatigue, which emerged as the primary contributors to cybersecurity fatigue among employees:

- (1) A key driver identified in the research was cybersecurity decision over-load, which was found to influence all three types of fatigue. The constant need to make security-related decisions led to mental exhaustion (cognitive fatigue), frustration with repetitive security actions (action-related fatigue) and the development of negative attitudes towards cybersecurity (attitudinal fatigue).
- (2) Workflow disruption also emerged as a significant factor, stemming from repetitive access requests and an overload of security checks. These frequent interruptions hindered productivity, manifesting action-related fatigue and resulting in attitudinal fatigue as employees grew increasingly frustrated with the intrusiveness of cybersecurity protocols.
- (3) Another contributing factor was work overload, which influenced cognitive and attitudinal fatigue. Within the SaaS organisation, employees frequently operate under dual-task conflict. Their cognitive capacity must be divided between primary, incentivised professional duties and other requirements. Employees often prioritised core work responsibilities over security-related tasks, perceiving cybersecurity measures as secondary or even obstructive, which negatively affected their cognitive focus and attitude.
- (4) The final factor identified was a poor understanding of risk, largely attributed to generic cybersecurity training and a lack of real-world examples. Without a clear

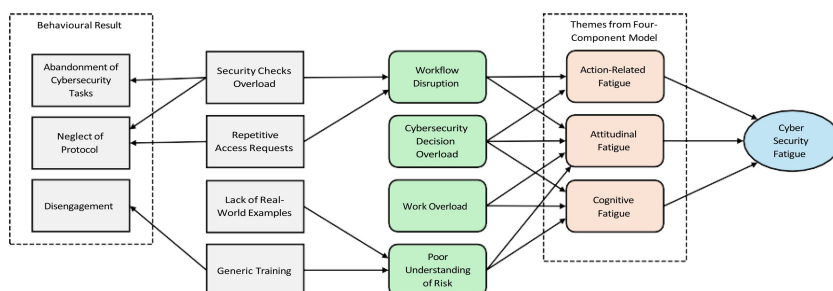


Figure 1. Conceptual model of cybersecurity fatigue

Source: Authors' own work

grasp of the potential consequences of cyber threats, employees failed to see the value of security protocols. This lack of understanding contributed to a perception of cybersecurity as burdensome, reinforcing cognitive and attitudinal fatigue.

Our thematic analysis did not show evidence indicative of advice-related fatigue and thus this construct is not included in the proposed conceptual model. Prior literature attributes such fatigue to excessive, inconsistent or overly complex security guidance, resulting in confusion, anxiety and eventual disengagement (Ogawa *et al.*, 2020; Reeves *et al.*, 2021; Bhana and Ophoff, 2023). These dynamics were not evident in the context of our case organisation. Instead, the challenges identified were primarily linked to the generic nature of the training provided and the absence of real-world examples. Rather than experiencing fatigue, participants appeared disengaged due to a perceived lack of relevance to their specific roles and a limited understanding of the practical consequences of security failures.

The model also addresses the second research question, proposing how cybersecurity fatigue manifests in observable, non-compliant workplace behaviours. Three behavioural outcomes were observed:

- (1) Employees were found to abandon tasks due to security checks overload. For example, the frustration of repetitive authentication is connected to abandonment of the HR platform (“I have to do the whole 2FA. I’m like, stuff this, I do not need this information”).
- (2) Employees frequently deviated from established security protocols when these were perceived as impeding their work. For example, prolonged ticketing approval delays encouraged deliberate workarounds (“In practice, I tend to just bug people [...] I need to do this to work, fix it”). Similarly, the requirement to change passwords every 30 days often resulted in superficial modifications, such as minor punctuation changes, rather than the adoption of substantially new passwords.
- (3) There was a clear disengagement from cybersecurity training, primarily resulting from training that was perceived as repetitive, generic and lacking relevance to employees’ specific roles (“I don’t think it adds much value, at least not for me”).

These fatigue-induced behaviours have significant implications for organisational security. By relying on unauthorised workarounds and disengaging from security training activities, employees inadvertently create human-centred vulnerabilities. This behavioural drift can undermine the effectiveness of otherwise robust security controls, generating knowledge gaps and procedural bypasses that increase the organisation’s exposure to accidental data breaches and external cyber threats.

5.1 Recommendations

By reinforcing the personal and organisational relevance of cybersecurity risks, companies can strengthen compliance and reduce the likelihood of fatigue-driven errors or negligence. A clear understanding of risk emerged as a potential solution to cybersecurity fatigue:

If you understand what that extra five seconds for MFA [multi-factor authentication] is protecting you against [...] your attitude towards it becomes positive. [P1]

I don’t think the training at companies really communicates the severity of the risks. People are focused on deadlines and job security, but a breach could cost a company so much more than a missed deadline. [P8]

The more important a user perceives a security task to be, the less likely they are to succumb to fatigue, even if the task requires significant effort (Furnell and Thomson, 2009). A limited understanding of risk contributes to cybersecurity fatigue by leading employees to perceive security measures as unnecessary burdens rather than essential safeguards. When employees are unaware of the potential consequences of security breaches, they are less likely to recognise the value of complying with requirements such as security checks, access requests and training initiatives.

Bridging the gap between awareness and understanding, especially through real-world examples, can shift employee attitudes, foster a positive security culture and mitigate fatigue. One participant reflected:

It used to be something that happens to other people or in the movies. It's a lot more real these days. [P2]

Employees who understand the direct impact of their actions on organisational security, and their own responsibilities, are more likely to appreciate and comply with security protocols.

5.1.1 Contextualised training with real-world relevance. The findings suggest that enhancing employees' understanding of cybersecurity risks is a key factor in fostering meaningful engagement with cybersecurity practices. One accessible and impactful strategy is to improve the quality and relevance of SETA. The research revealed that a major reason employees disengage from cybersecurity training is its overly generic nature. Therefore, tailoring SETA to specific roles is a critical first step in strengthening employees' risk perception.

Further investigation is needed to determine which training elements should be adapted to increase relevance and engagement. A promising approach is the integration of real-world examples directly aligned with employees' roles. This would make potential threats more tangible and relevant, thereby increasing the perceived value of cybersecurity protocols.

In addition, alternative delivery formats may enhance engagement. For example, in-person workshops, as suggested by one participant, could replace passive video-based training. Activities such as cybersecurity "war games" may encourage active participation by creating interactive learning environments that simulate real incidents. The social and collaborative nature of such workshops, especially when attended by peers and supervisors, can further boost motivation and accountability. Other innovative tools include the use of card games to raise awareness of social engineering attacks (Shostack, 2014; Beckers and Pape, 2016). These interactive methods not only improve knowledge retention and decision-making skills but also promote collaboration and a culture of shared responsibility (Aldawood and Skinner, 2019).

5.1.2 Streamlining security processes. Another key recommendation is the simplification and acceleration of security processes. In our case organisation this can be tied to access request tickets. Delays in access approval, sometimes extending over several days, were shown to be a source of frustration, contributing to attitudinal fatigue and encouraging employees to bypass formal procedures.

Reducing the wait time for access requests could mitigate this frustration and increase adherence to protocol. When employees perceive security processes as efficient and reasonable, they are more likely to comply rather than seek informal workarounds, such as requesting favours from colleagues. This shift in behaviour would strengthen organisational security and reduce the risk of unauthorised access, ultimately supporting a more resilient cybersecurity culture.

5.2 Limitations

This study explored the factors contributing to cybersecurity fatigue among employees in a cloud computing organisation and examined how these factors influence employee behaviour. However, several limitations must be acknowledged. The research was conducted

over a short timeframe and focused on a single case study. The concepts of generalisability and saturation are frequently debated in interpretivist qualitative research and are not the aims of our study. Accordingly, we do not claim to have achieved them. Braun *et al.* (2019) suggested that a small, focused study involving a relatively homogenous sample may be appropriately conducted with as few as five or six interviews. Although eight participants were interviewed a larger sample size could provide deeper insight into the phenomenon. Future research could expand the scope by including multiple organisations across different industries and adopting a longitudinal design to enhance data quality and capture changes in employee experiences over time. Using a quantitative approach in these investigations would support broader generalisability and comparative analysis.

6. Conclusion

This study investigated the causes and behavioural impacts of cybersecurity fatigue among employees of a cloud computing provider, an area that has received limited attention despite the increasing reliance on SaaS operations. The findings identified four main contributors to cybersecurity fatigue: cybersecurity decision overload, workflow disruption, work overload and a poor understanding of risk. Frequent and critical security decision-making, repetitive processes (such as access requests and 2FA), and the prioritisation of work deadlines over security tasks all contributed to fatigue and frustration. In addition, generic training and a lack of real-world context diminished employees' understanding of cybersecurity risks, reinforcing negative attitudes towards security protocols.

The study also uncovered three key behavioural outcomes: abandonment of security tasks, neglect of proper protocol and disengagement from training. These behaviours increase organisational vulnerability to cyber threats. In response, we recommend two strategies: implementing contextualised, role-specific training using real-world examples and streamlining security processes to reduce delays and workflow disruption.

Future research should further investigate attitudinal fatigue, a key contributor to cybersecurity fatigue identified in this study. When employees perceive cybersecurity measures as irrelevant or burdensome, their negative attitudes can lead to disengagement and non-compliance, increasing organisational vulnerability to cyber-attacks. The conceptual model offers a foundation for exploring how to design more engaging, role-relevant training programs that promote positive employee attitudes towards cybersecurity. In addition, the model could be integrated into behavioural analytic systems to monitor employee engagement and identify points where disengagement occurs, guiding targeted interventions.

Acknowledgements

The authors thank the case organisation and its employees for their participation in this study. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Note

[1.] <https://lumivero.com/products/nvivo/>

References

Acuña, D. (2016), "Effects of a comprehensive computer security policy on computer security culture", *MWAIS 2016 Proceedings*, available at: <https://aisel.aisnet.org/mwais2016/10/>

- Aldawood, H. and Skinner, G. (2019), "Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues", *Future Internet*, Vol. 11 No. 3, p. 73, doi: [10.3390/fi11030073](https://doi.org/10.3390/fi11030073).
- Alotaibi, M., Furnell, S. and Clarke, N. (2016), "Information security policies: a review of challenges and influencing factors", *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 352-358, doi: [10.1109/ICITST.2016.7856729](https://doi.org/10.1109/ICITST.2016.7856729).
- Ament, C. and Haag, S. (2016), "How information security requirements stress employees", *ICIS 2016 Proceedings*, available at: <https://aisel.aisnet.org/icis2016/ISSecurity/Presentations/9>
- Arce, D.G. (2020), "Cybersecurity and platform competition in the cloud", *Computers and Security*, Vol. 93, p. 101774, doi: [10.1016/j.cose.2020.101774](https://doi.org/10.1016/j.cose.2020.101774).
- Beckers, K. and Pape, S. (2016), "A serious game for eliciting social engineering security requirements", *2016 IEEE 24th International Requirements Engineering Conference*, pp. 16-25, doi: [10.1109/RE.2016.39](https://doi.org/10.1109/RE.2016.39).
- Bhana, A. and Ophoff, J. (2023), "Risk homeostasis and security fatigue: a case study of data specialists", *Information and Computer Security*, Vol. 31 No. 3, pp. 267-280, doi: [10.1108/ICS-11-2022-0172](https://doi.org/10.1108/ICS-11-2022-0172).
- Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: [10.1191/1478088706qp0630a](https://doi.org/10.1191/1478088706qp0630a).
- Braun, V., Clarke, V., Hayfield, N. and Terry, G. (2019), "Thematic analysis", in Liamputtong, P. (Ed.), *Handbook of Research Methods in Health Social Sciences*, Springer, Singapore, pp. 843-860, doi: [10.1007/978-981-10-5251-4_103](https://doi.org/10.1007/978-981-10-5251-4_103).
- Clarke, V. and Braun, V. (2017), "Thematic analysis", *The Journal of Positive Psychology*, Vol. 12 No. 3, pp. 297-298, doi: [10.1080/17439760.2016.1262613](https://doi.org/10.1080/17439760.2016.1262613).
- Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2021), "When enough is enough: investigating the antecedents and consequences of information security fatigue", *Information Systems Journal*, Vol. 31 No. 4, pp. 521-549, doi: [10.1111/isj.12319](https://doi.org/10.1111/isj.12319).
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. (2022), "Cyber risk and cybersecurity: a systematic review of data availability", *The Geneva Papers on Risk and Insurance – Issues and Practice*, Vol. 47 No. 3, pp. 698-736, doi: [10.1057/s41288-022-00266-6](https://doi.org/10.1057/s41288-022-00266-6).
- D'Arcy, J., Tejaswini, H. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285-318, doi: [10.2753/MIS0742-1222310210](https://doi.org/10.2753/MIS0742-1222310210).
- Davis, J., Agrawal, D. and Guo, X. (2023), "Enhancing users' security engagement through cultivating commitment: the role of psychological needs fulfilment", *European Journal of Information Systems*, Vol. 32 No. 2, pp. 195-206, doi: [10.1080/0960085X.2021.1927866](https://doi.org/10.1080/0960085X.2021.1927866).
- De Vos, S., Crouch, R., Quester, P. and Ilicic, J. (2017), "Examining the effective-ness of fear appeals in prompting help-seeking: the case of at-risk gamblers", *Psychology and Marketing*, Vol. 34 No. 6, pp. 648-660, doi: [10.1002/mar.21012](https://doi.org/10.1002/mar.21012).
- Dykstra, J. and Paul, C.L. (2018), "Cyber operations stress survey (COSS): studying fatigue, frustration, and cognitive workload in cybersecurity operations", available at: www.usenix.org/conference/cset18/presentation/dykstra (accessed 2 April 2025).
- Eling, M. and Schnell, W. (2016), "What do we know about cyber risk and cyber risk insurance?", *The Journal of Risk Finance*, Vol. 17 No. 5, pp. 474-491, doi: [10.1108/JRF-09-2016-0122](https://doi.org/10.1108/JRF-09-2016-0122).
- Furnell, S. and Thomson, K.-L. (2009), "Recognising and addressing 'security fatigue'", *Computer Fraud and Security*, Vol. 2009 No. 11, pp. 7-11, doi: [10.1016/S1361-3723\(09\)70139-3](https://doi.org/10.1016/S1361-3723(09)70139-3).
- Gerdenitsch, C., Wurhofer, D. and Tscheligi, M. (2023), "Working conditions and cybersecurity: time pressure, autonomy and threat appraisal shaping employees' security behavior", *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 17 No. 4, doi: [10.5817/CP2023-4-7](https://doi.org/10.5817/CP2023-4-7).

- Glaspie, H.W. and Karwowski, W. (2018), "Human factors in information security culture: a literature review", in Nicholson, D. (Ed.), *Advances in Human Factors in Cybersecurity*, Springer International Publishing, Cham, pp. 269-280, doi: [10.1007/978-3-319-60585-2_25](https://doi.org/10.1007/978-3-319-60585-2_25).
- Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G. and Koshutanski, H. (2020), "Modern aspects of cyber-security training and continuous adaptation of programmes to trainees", *Applied Sciences*, Vol. 10 No. 16, p. 5702, doi: [10.3390/app10165702](https://doi.org/10.3390/app10165702).
- Haynes, G.A. (2009), "Testing the boundaries of the choice overload phenomenon: the effect of number of options and time pressure on decision difficulty and satisfaction", *Psychology and Marketing*, Vol. 26 No. 3, pp. 204-212, doi: [10.1002/mar.20269](https://doi.org/10.1002/mar.20269).
- Herley, C. (2009), "So long, and No thanks for the externalities: the rational rejection of security advice by users", *Proceedings of the 2009 Work-shop on New Security Paradigms Workshop*, pp. 133-144, doi: [10.1145/1719030.1719050](https://doi.org/10.1145/1719030.1719050).
- Howarth, J. (2024), "How many SaaS companies are there? (2024)", Exploding Topics, available at: <https://explodingtopics.com/blog/number-of-saas-companies> (accessed 3 April 2025).
- Hsu, J.S.-C., Hung, Y.W., Hsieh, P.-J. and Chiu, C.-M. (2024), "Examining formation and alleviation of information security fatigue by using job demands-resources theory", *Information Systems Journal*, Vol. 34 No. 6, pp. 2132-2172, doi: [10.1111/isj.12524](https://doi.org/10.1111/isj.12524).
- Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-660, doi: [10.1111/j.1540-5915.2012.00361.x](https://doi.org/10.1111/j.1540-5915.2012.00361.x).
- Hughes-Lartey, K., Li, M., Botchey, F.E. and Qin, Z. (2021), "Human factor, a critical weak point in the information security of an organization's internet of things", *Heliyon*, Vol. 7 No. 3, p. e06522, doi: [10.1016/j.heliyon.2021.e06522](https://doi.org/10.1016/j.heliyon.2021.e06522).
- Hull, J. (2017), "Analyst burnout in the Cyber Security Operation Center – CSOC: a phenomenological study – ProQuest", available at: www.proquest.com/openview/1c3f22fb52de7b293c9b4aabadbab815/ (accessed 2 April 2025).
- Humayun, M., Niazi, M., Almufareh, M.F., Jhanjhi, N.Z., Mahmood, S. and Al-Shayeb, M. (2022), "Software-as-a-service security challenges and best practices: a multivocal literature review", *Applied Sciences*, Vol. 12 No. 8, p. 3953, doi: [10.3390/app12083953](https://doi.org/10.3390/app12083953).
- IBM (2024), "Cost of a data breach 2024", available at: www.ibm.com/reports/data-breach (accessed 2 April 2025).
- ISACA (2020), "Industry news 2020 understanding and addressing CISO burnout", ISACA, available at: www.isaca.org/resources/news-and-trends/industry-news/2020/understanding-and-addressing-ciso-burnout (accessed 2 April 2025).
- Jiang, R. and Zhang, J. (2023), "The impact of work pressure and work completion justification on intentional nonmalicious information security policy violation intention", *Computers and Security*, Vol. 130, p. 103253, doi: [10.1016/j.cose.2023.103253](https://doi.org/10.1016/j.cose.2023.103253).
- Johnston, A.C., Warkentin, M., Dennis, A.R. and Siponen, M. (2019), "Speak their language: designing effective messages to improve employees' information security decision making", *Decision Sciences*, Vol. 50 No. 2, pp. 245-284, doi: [10.1111/deci.12328](https://doi.org/10.1111/deci.12328).
- Montañez, R., Golob, E. and Xu, S. (2020), "Human cognition through the lens of social engineering cyberattacks", *Frontiers in Psychology*, Vol. 11, doi: [10.3389/fpsyg.2020.01755](https://doi.org/10.3389/fpsyg.2020.01755).
- Moustafa, A.A., Bello, A. and Maurushat, A. (2021), "The role of user behaviour in improving cyber security management", *Frontiers in Psychology*, Vol. 12, doi: [10.3389/fpsyg.2021.561011](https://doi.org/10.3389/fpsyg.2021.561011).
- Nobles, C. (2022), "Stress, burnout, and security fatigue in cybersecurity: a human factors problem", *HOLISTICA – Journal of Business and Public Administration*, Vol. 13 No. 1, pp. 49-72, doi: [10.2478/hjbpa-2022-0003](https://doi.org/10.2478/hjbpa-2022-0003).

- Norton, C., Ruhwanya, Z. and Ophoff, J. (2026), "Factors contributing to cybersecurity fatigue", in Furnell, S. and Clarke, N. (Eds), *Human Aspects of Information Security and Assurance*, Springer Nature Switzerland, Cham, pp. 198-211, doi: [10.1007/978-3-032-02504-3_14](https://doi.org/10.1007/978-3-032-02504-3_14).
- Nowell, L.S., Norris, J.M., White, D.E. and Moules, N.J. (2017), "Thematic analysis: striving to meet the trustworthiness criteria", *International Journal of Qualitative Methods*, Vol. 16 No. 1, p. 1609406917733847, doi: [10.1177/1609406917733847](https://doi.org/10.1177/1609406917733847).
- Nurse, J.R.C., Milward, J. and Alashe, O. (2025), "From security awareness and training to human risk management in cybersecurity", in Moallem, A. (Ed.), *HCI for Cybersecurity, Privacy and Trust*, Springer Nature Switzerland, Cham, pp. 86-104, doi: [10.1007/978-3-031-92833-8_6](https://doi.org/10.1007/978-3-031-92833-8_6).
- Ogawa, M., Tanimoto, S., Hatashima, T. and Kanai, A. (2020), "Information security fatigue countermeasures based on cognitive strategy scale", *2020 Eighth International Symposium on Computing and Networking Work-shops*, pp. 362-367, doi: [10.1109/CANDARW51189.2020.00075](https://doi.org/10.1109/CANDARW51189.2020.00075).
- Palos-Sanchez, P.R., Arenas-Marquez, F.J. and Aguayo-Camacho, M. (2017), "Cloud computing (SaaS) adoption as a strategic technology: results of an empirical study", *Mobile Information Systems*, Vol. 2017, No. 1, p. 2536040, doi: [10.1155/2017/2536040](https://doi.org/10.1155/2017/2536040).
- Pfleeger, S.L. and Caputo, D.D. (2012), "Leveraging behavioral science to mitigate cyber security risk", *Computers and Security*, Vol. 31 No. 4, pp. 597-611, doi: [10.1016/j.cose.2011.12.010](https://doi.org/10.1016/j.cose.2011.12.010).
- 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*, Vol. 46, pp. 96-107, doi: [10.1016/j.jisa.2019.03.012](https://doi.org/10.1016/j.jisa.2019.03.012).
- Posey, C., Bennett, R.J., Roberts, T.L. and Lowry, P.B. (2011), "When computer monitoring backfires: privacy invasions and organizational injustice as precursors to computer abuse", *Journal of Information Systems Security*, Vol. 7 No. 1, pp. 24-47, available at: www.jissec.org/Contents/V7/N1/V7N1-Posey.html (accessed 3 April 2025).
- Rahman, A. and Pribadi Subriadi, A. (2022), "Software as a service (SaaS) adoption factors: individual and organizational perspective", *2022 2nd International Conference on Information Technology and Education*, pp. 31-36, doi: [10.1109/ICITE54466.2022.9759891](https://doi.org/10.1109/ICITE54466.2022.9759891).
- Rath, A., Spasic, B., Boucart, N. and Thiran, P. (2019), "Security pattern for cloud SaaS: from system and data security to privacy case study in AWS and azure", *Computers*, Vol. 8 No. 2, p. 34, doi: [10.3390/computers8020034](https://doi.org/10.3390/computers8020034).
- Reeves, A., Delfabbro, P. and Calic, D. (2021), *Encouraging Employee Engage-Ment With Cybersecurity: How to Tackle Cyber Fatigue*, SAGE Open, SAGE Publications, Los Angeles, CA, doi: [10.1177/21582440211000049](https://doi.org/10.1177/21582440211000049).
- Reeves, A., Calic, D. and Delfabbro, P. (2023), "Generic and unusable"1: understanding employee perceptions of cybersecurity training and measuring advice fatigue", *Computers and Security*, Vol. 128, p. 103137, doi: [10.1016/j.cose.2023.103137](https://doi.org/10.1016/j.cose.2023.103137).
- Reeves, A., Calic, D. and Delfabbro, P. (2025), "How to De-CyFa the actor-observer bias in cybersecurity fatigue: building the CyFa measure of attribution styles and mitigation strategies", *Computers and Security*, Vol. 150, p. 104179, doi: [10.1016/j.cose.2024.104179](https://doi.org/10.1016/j.cose.2024.104179).
- Robinson, N. (2023), "Human factors security engineering: the future of cyber-security teams", *EDPACS*, Vol. 67 No. 5, pp. 1-17, doi: [10.1080/07366981.2023.2211429](https://doi.org/10.1080/07366981.2023.2211429) (accessed 2 April 2025).
- Rocha Flores, W., Antonsen, E. and Ekstedt, M. (2014), "Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture", *Computers and Security*, Vol. 43, pp. 90-110, doi: [10.1016/j.cose.2014.03.004](https://doi.org/10.1016/j.cose.2014.03.004).
- Safa, N.S., Von Solms, R. and Fletcher, L. (2016), "Human aspects of information security in organisations", *Computer Fraud and Security*, Vol. 2016 No. 2, pp. 15-18, doi: [10.1016/S1361-3723\(16\)30017-3](https://doi.org/10.1016/S1361-3723(16)30017-3).

- Sheridan, K. (2020), "90% Of CISOs would cut pay for better work-life balance", available at: www.darkreading.com/cyber-risk/90-of-cisos-would-cut-pay-for-better-work-life-balance (accessed 2 April 2025).
- Shostack, A. (2014), "Elevation of privilege: drawing developers into threat modeling", available at: www.usenix.org/conference/3gse14/summit-program/presentation/shostack (accessed 3 April 2025).
- Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S. (2016), "Security fatigue", *IT Professional*, Vol. 18 No. 5, pp. 26-32, doi: [10.1109/MITP.2016.84](https://doi.org/10.1109/MITP.2016.84).
- Sun, J.C.-Y. and Lee, K.-H. (2016), "Which teaching strategy is better for enhancing anti-phishing learning motivation and achievement?: The concept maps on tablet PCs or worksheets?", *Journal of Educational Technology and Society*, Vol. 19 No. 4, pp. 87-99, available at: www.jstor.org/stable/jeductechsoci.19.4.87 (accessed 3 April 2025).
- Tarafdar, M., Tu, Q., Ragu-Nathan, B.S. and Ragu-Nathan, T.S. (2007), "The impact of technostress on role stress and productivity", *Journal of Management Information Systems*, Vol. 24 No. 1, pp. 301-328, doi: [10.2753/MIS0742-1222240109](https://doi.org/10.2753/MIS0742-1222240109).
- Thomas, J. (2018), "Individual cyber security: empowering employees to resist spear phishing to prevent identity theft and ransomware attacks", *International Journal of Business and Management*, Vol. 13 No. 6, p. 1, doi: [10.5539/ijbm.v13n6p1](https://doi.org/10.5539/ijbm.v13n6p1).
- Vance, A., Jenkins, J.L., Anderson, B.B., Bjornn, D.K. and Kirwan, C.B. (2018), "Tuning out security warnings: a longitudinal examination of habituation through fMRI, eye tracking, and field Experiments1", *MIS Quarterly*, Vol. 42 No. 2, pp. 355-380, doi: [10.25300/MISQ/2018/14124](https://doi.org/10.25300/MISQ/2018/14124).
- Yang, Z., Saini, R. and Freling, T. (2015), "How anxiety leads to suboptimal decisions under risky choice situations", *Risk Analysis*, Vol. 35 No. 10, pp. 1789-1800, doi: [10.1111/risa.12343](https://doi.org/10.1111/risa.12343).

Corresponding author

Zainab Ruhwanya can be contacted at: zainab.ruhwanya@uct.ac.za