Review Article

SAGE Open
January-March 2021: 1–18
© The Author(s) 2021
DOI: 10.1177/21582440211000049
journals.sagepub.com/home/sgo
SAGE

Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue

A. Reeves[1], P. Delfabbro[1], and D. Calic[2]

Abstract

Cybersecurity fatigue is a form of work disengagement specific to cybersecurity. It manifests as a weariness or aversion to cybersecurity-related workplace behaviors or advice and occurs as a result of prior overexposure to cybersecurity-related work demands or training. While some previous theoretical conceptualizations of cybersecurity fatigue are available, this article is the first to capture all dimensions of the phenomenon in a four-component model. The model holds that cybersecurity fatigue can result from overexposure to workplace cybersecurity advice (e.g., training) or cybersecurity actions (e.g., forced password updates). Similarly, we argue that there can be two types of cybersecurity fatigue: attitudinal (e.g., a belief that cybersecurity is not important) and cognitive (e.g., habituated bad behaviors). We present a multidisciplinary review, which draws on research from management, psychology, and information systems. Practitioners can use the four-component model to identify the type of cybersecurity fatigue that may be occurring in employees and adapt workplace processes accordingly to improve behavior. In addition, we present three illustrative case studies, adapted from employee experiences, to demonstrate the application of the four-component model to an organizational context. The review presents a framework for coordinating the existing approaches to cybersecurity fatigue in the current literature.

Keywords

cyber security, fatigue, disengagement, human aspects, information security

Introduction

In 2018, 35% of Chief Cyber Security Officers reported employee security education and training as the highest priority to ensure cyber security, outweighing infrastructure upgrades, breach defense, and network defense (Financial Services Information Sharing and Analysis Center, 2018). To facilitate this, organizations have invested in security education, training, and awareness (SETA) programs for their employees (Coventry et al., 2014; Telstra Corporation, 2018). SETA programs typically aim to educate employees on what are acceptable cyber security behaviors and emphasize the consequences should they not maintain these behaviors (D'Arcy et al., 2009). Such programs are often ineffective as the relationship between the amount of cyber security training an employee has had, and their ability to avoid a cyber threat, is often not very strong (Pattinson et al., 2016b). Moreover, the relationship is occasionally negative. For example, Parsons et al. (2013) found that individuals who had received more frequent formal cyber security training were less likely to correctly distinguish between phishing and legitimate emails than those who had received less frequent training. Similarly, Pattinson et al. (2016a) found that individuals who had received formal cyber security training outside of their workplace had poorer awareness of cyber security risks than others. These results suggest that, rather than reducing the risk to businesses, SETA programs may have the potential to deteriorate the cyber security behavior of employees.

In this article, we argue that one reason for these findings is that employees become fatigued. For example, employees may find that the actions required to maintain cyber security are overwhelming and tiresome and, as a result, they disengage from security-related behavior (Furnell & Thomson, 2009). The article commences with a discussion of the evidence that has led to a need to investigate cyber security fatigue. In a second section, we provide a definition of cyber security fatigue, which we use to identify relevant literature

[1]The University of Adelaide, SA, Australia
[2]Defence Science and Technology, Edinburgh, SA, Australia

Corresponding Author:
A. Reeves, School of Psychology, The University of Adelaide, Hughes Building, North Terrace, Adelaide, SA 5005, Australia.
Email: andrew.reeves@adelaide.edu.au

for review. Using this material, we describe the dimensions of cyber security fatigue and join these into a four-component model. Finally, we demonstrate how to use the four-component model via three illustrative case studies.

The Case for Fatigue

Some researchers have suggested that employee overconfidence and complacency can explain the negative relationship between cyber security training frequency and workplace behaviors (K. Parsons et al., 2013; Pattinson et al., 2016a; Reeves et al., 2020). Employees may feel that, following training, they are well equipped to deal with cyber security threats and are, therefore, less vulnerable. As a result, they may become careless in their day-to-day security-related behaviors. However, if complacency was the sole-contributing factor, targeted SETA programs that aim to instill greater awareness should be successful in reducing complacency. In many instances, this is not the case (Pattinson et al., 2016a; Reeves et al., 2020). Instead, suboptimal employee behavior is better explained as a result of fatigue. SETA programs can add to this fatigue by making employees feel overwhelmed, frustrated, and tired of hearing about cyber security (Stanton et al., 2016). This leads them to no longer engage with cyber security advice (D'Arcy et al., 2014) and to disregard security-related protocols (Choi & Jung, 2018).

Following a method advocated by Madden et al. (2018), we conducted a narrative review of the available literature. This approach is appropriate given that the topic of cyber security fatigue does not, as yet, have the level of coherency or consistency necessary for a systematic review of comparable studies (Denise et al., 2012; Madden et al., 2018). Drawing on relevant literature, we define cyber security fatigue as a weariness, aversion, or manifested lack of motivation in regard to cyber security, which exists not solely as a result of individual predispositions but primarily because of prior overexposure to cyber security (training or related workplace demands) or a lack of available cognitive or workplace resources.

We considered material to be relevant to our review if it related to: (a) tiredness with, and aversion to, technologies, where the technology related to cyber security or (b) workplace fatigue and aversion to workplace duties related to cyber security. We found that approaches to cyber security fatigue could be broadly described by two components: Factors relating to employee attitude (e.g., reactance) and factors that are cognitive and largely unconscious (e.g., habituation). In addition, we argue that the precursors of fatigue are either advice-related (e.g., frequent SETA programs) or action-related (e.g., high workplace demands). Our model, therefore, consists of two broad categories, each containing two components. Combining these two categories forms the four-component model of cyber security fatigue. Table 1 summarizes the evidence in support of the identified components. Table 1 also summarizes seven contributing factors of cyber security fatigue and their underlying processes. Practitioners can refer to a schematic presented in Table 1 to identify what type of fatigue is present in their workforce, what processes may be responsible, and what actions the four-component model recommends.

The Four-Component Model

The recommendations for dealing with the problem of cyber security fatigue are often contradictory. Some authors have suggested that due to the increased chance of people adopting technologies, they have control over (Kroenung & Eckhardt, 2015; Zolotov et al., 2018), or when they have assisted in the decision-making process (Tarafdar et al., 2010), cyber security practitioners can ease employee fatigue by allowing employees to have greater agency of their cyber security behaviors (Lowry & Moody, 2015). However, doing so increases the decision-making load on the employee, which may itself be fatiguing. Therefore, in an effort to reduce the cognitive load on the employee, some have suggested taking the decision-making ability away wherever possible (Stanton et al., 2016). However, employees may view this as an infringement on their self-determination, leading to pernicious behavior (Lowry & Moody, 2015). Accordingly, to unify these conflicting approaches to cyber security fatigue, we propose a model that comprises four components of fatigue across two categories. The first category of fatigue source holds that fatigue can be advice- or action-related. The second category of fatigue type holds that fatigue can appear as attitudinal or cognitive. Each component may operate independently or interrelate with each other, depending on the circumstance. Figure 1 presents a diagram of the four-component model.

Fatigue Type: Cognitive or Attitudinal

The first category, fatigue type refers to the two ways in which individuals will experience and manifest cyber security fatigue. Attitudinal-type fatigue is where an individual has a negative effect relating to cyber security (e.g., Ayyagari, 2008). This fatigued attitude can include feelings of emotional exhaustion (Choi & Jung, 2018), moral disengagement (i.e., a tendency to no longer care about doing the right thing; D'Arcy et al., 2014), and cynicism, both regarding the value of cyber security and of their ability to cope with its demands (Choi & Jung, 2018; Stanton et al., 2016). By contrast, cognitive-type fatigue refers to the limited capacity individuals have to make decisions (Hickman et al., 2018), or to cope with increased cognitive load (Vohs et al., 2008). In situations where employees have depleted their cognitive resources, they will fall back on impulsive, intuitive, and biased decision-making, or avoid the decision entirely (Danziger et al., 2011). In the case of cyber security, this could mean dismissing security warnings or basing trust in the legitimacy of emails to a gut-reaction. Our model holds

Table 1. Literature Relevant to Cybersecurity Fatigue Within the Four-Component Model.

Contributing factor	Fatigue source	Process	Key reference	Discipline	Applied recommendations
Cognitive-type fatigue					
Depletion	Action-related	Repetitive decision-making High or constant workload	Pignatiello et al. (2020); Pfleeger and Caputo (2012)	Cognitive Psychology	[3]Efforts to activate systematic thinking in regard to cyber security may be unsuccessful. Focus should be on reducing depletion.
Habituation of actions	Action-related	Repetitive decision-making	Amran et al. (2018)	Information systems	Habituation reduction strategies should consider unintended attitudinal consequences.
Habituation to advice/messaging	Advice-related	Repetitive, constant information	Stanton et al. (2016)	Information systems	Attempts to reduce habituation may have the unintended consequence of employee frustration and lead to poor attitudes to cyber security.
Attitudinal-type fatigue					
Moral disengagement	Action or advice related	Breach fatigue; emotion-focused coping Diffusion of responsibility	Reitberger and Wetzel (2017)	Information systems	Employee behavior may be due to information overload. Keep messaging centralized, simple, and consistent.
Reactance	Advice-related	Trait reactance; Perceived threat to freedom	D'Arcy et al. (2009); Brehm (1966)	Information systems Psychology	[1]Assess whether employees are likely to perceive that new cyber security systems are a threat to their freedom.
Poor perception of cost and benefits	Action or advice related	Low threat appraisal; Low perceived ease of use/ compliance; Low perceived utility; High internal coping appraisal.	Lowry and Moody (2015); Furnell and Thomson (2009); Liang and Xue (2009)	Information systems Information systems /organizational psychology Information systems	Simplify security-related systems and processes. Raise employee threat appraisal.
Burnout	Action or advice related	Technostress; overwhelming information/workplace demands	Brod (1982); Atanasoff and Venable (2017); D'Arcy et al. (2014).	Management Management Management/ information systems	[2]Do not assume burnout is the result of cyber security actions. Identify the source of the fatigue.

Note. [1,2,3]Respectively, case studies 1, 2, and 3 provide an illustrative example of these recommendations (p. 24).

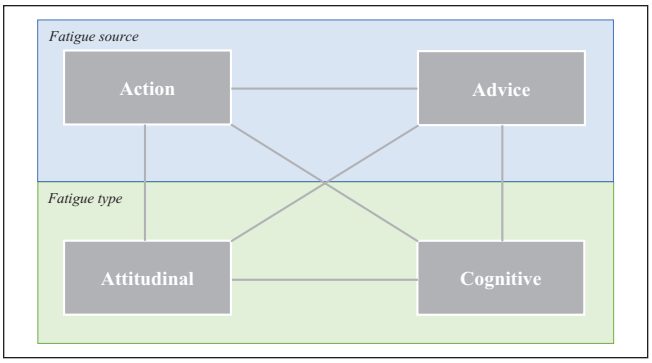

Figure 1. The four-component model of cyber security fatigue.

that cognitive-type fatigue is related to the internal state of the employee at the moment that an action is taken and is therefore somewhat transient (e.g., different decisions may be made when an individual is alert at the commencement of a workday compared with when they are exhausted at the end of the day). Employees can reduce their cognitive-type fatigue by simply taking breaks or by focusing on a different task for a period of time (Hagger et al., 2010). In contrast, attitudinal-type fatigue is more enduring, and in this way somewhat akin to a "trait" (Ormond et al., 2019). While it may be possible to reduce attitudinal-type fatigue with intervention, we see this type of fatigue as less transient due to observations from research that attitudes, once set, are difficult to change (see Bada et al., 2019 for a review). Examples of cognitive-type fatigue include ego depletion (Dang, 2018) and decision fatigue (Pignatiello et al., 2020), while examples of attitudinal-type fatigue include reactance (Lowry & Moody, 2015) and moral disengagement (D'Arcy et al., 2014).

Fatigue Source: Action or Advice

As with fatigue type, fatigue source is also viewed as a pair. We use this term to refer to the aspect of overexposure that is the cause of the fatigue, that is, are employees fatigued with the advice about cyber security they receive, or are they simply tired of performing the behaviors required to maintain cyber security? For example, an employee who is tired of being told what to do may express exhaustion at the very mention of cyber security or a new cyber security policy. In this sense, their fatigue is advice-related. By contrast, if an employee is tired of having to change at least one system password every few days, or having to decide whether each email they receive is legitimate or not, their fatigue stems from the often-repetitive actions required to maintain cyber security. In this sense, their fatigue is action-related. Examples of action-related fatigue include when arduous authentication prompts deplete employees' cognitive resources and lead to unsecure behaviors (e.g., Groß et al., 2019), or when cumbersome multifactor authentication systems frustrate employees and reduce compliance motivation (e.g., Das et al., 2020). The former is an example of an action-related source leading to cognitive-type fatigue, whereas the latter is an example of an action-related source leading to attitudinal-type fatigue.

Our model holds that each type of fatigue can be caused by either source of fatigue, that is, attitudinal-type fatigue can result from an overexposure to poorly conceived cybersecurity advice, or, equally, from an overexposure to cybersecurity actions and workplace demands. For example, employees may become cynical about cyber security (an attitudinal manifestation of fatigue) either because the advice they receive is overly complex or confusing (an advice-related source of fatigue), or, because the actions they must take to maintain their cyber security are equally complex or confusing (an action-related source of fatigue). Similarly, in some instances, cognitive-type fatigue can result from either cybersecurity actions (such as habituation to repetitive system warning prompts), or, cybersecurity advice (such as habituation to repetitive cyber security advice).

Both sources of fatigue are problematic and, crucially for business, both will likely have similar outcomes in terms of poor behaviors. It is also likely that both advice and action simultaneously can fatigue employees, requiring cyber security managers to address both. Figure 2 provides a summary of the four components with concrete illustrations of each taken from employee sentiments recorded as part of this project (Reeves et al., 2020a).

These distinctions have important implications for interventions. An employee who is experiencing attitudinal-type fatigue may be unmoved by an intervention, which seeks to reduce the cognitive load required to maintain cyber security. For example, an employee who does not see the value in maintaining cyber security (attitudinal-type fatigue) will likely not comply with the cyber security policy of their organization, even if the policy is simplified (reduced action-related fatigue). In the same vein, an intervention that seeks to improve the attitude of employees regarding cyber security will likely be ineffective if the cyber security demands placed on the individual remain impossible to achieve (Stanton et al., 2016). Consequently, both attitudinal and cognitive types of fatigue are important to consider when addressing cyber security fatigue.

The following sections provide a more detailed analysis of each component and the specific mechanism to explain how they are inter-related. They focus on the seven factors identified in the literature, which contribute to the attitudinal and cognitive types of cyber security fatigue, and discuss how each factor can be caused by an action-related source, an advice-related source, or in some instances, either source. This discussion is not intended to be an exhaustive list of all factors available in the literature. Rather, this section organizes and interprets existing literature through the lense of the four-component model. Furthermore, we discuss the presented factors from an applied implications and future research perspectives.

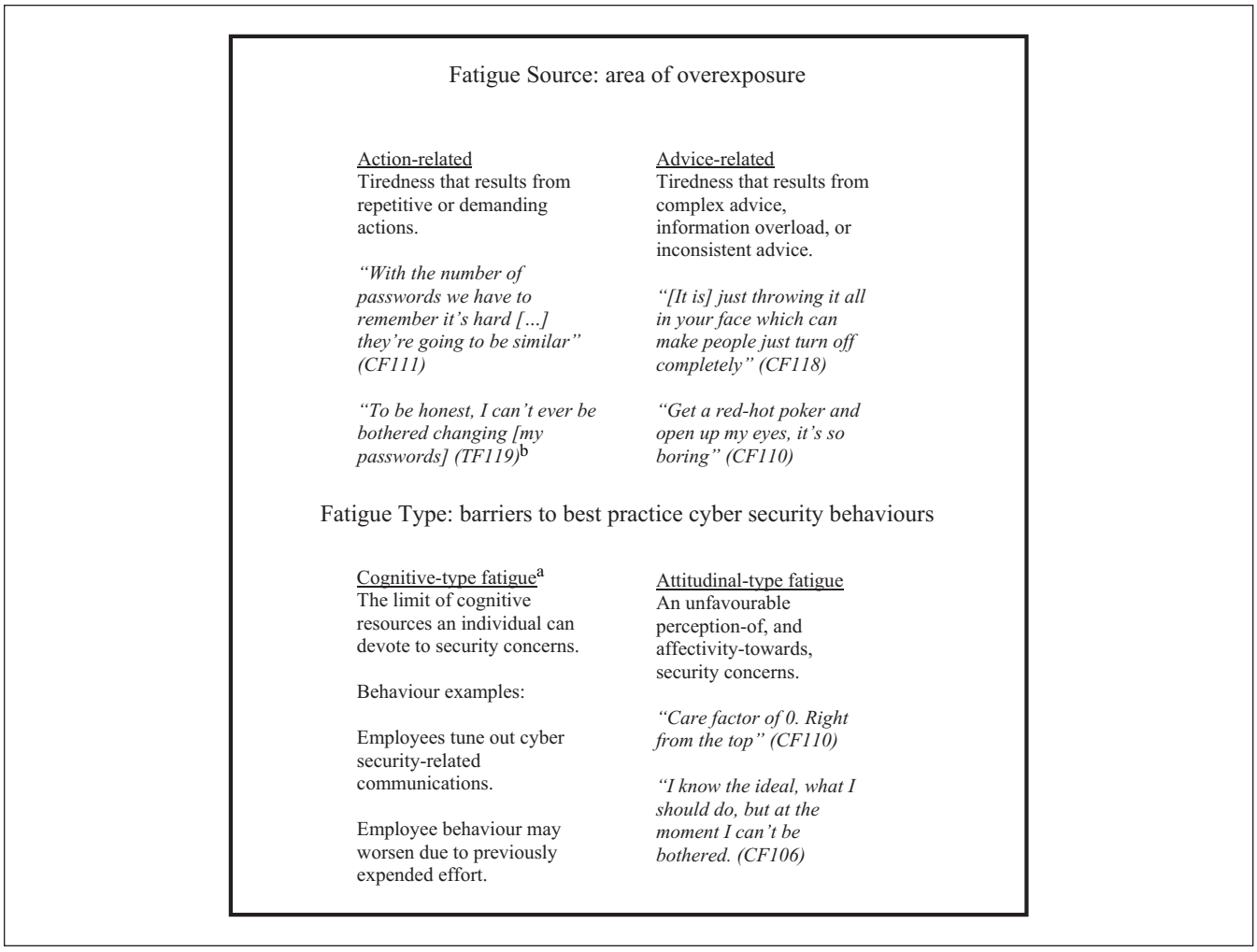

Figure 2. The four-component model of cyber security fatigue with examples of employee sentiment taken from Reeves et al. (2020a), shown in italics.
[a]Quotes are not provided as some forms of cognitive-type fatigue are not consciously salient and may not be openly expressed in interviews.
[b]Parentheses contain participant identifiers.

Cognitive-Type Fatigue

When an employee appears fatigued regarding cyber security (e.g., creating weak passwords, or not recognizing a phishing email), their behavior is often attributed to their attitude (e.g., Choi & Jung, 2018; Furnell & Thomson, 2009; Lowry & Moody, 2015; Stanton et al., 2016). SETA programs often, therefore, tend to focus on improving attitudes. However, such approaches, and many others, may not fully consider the limitations of human cognitive ability, and its role in fatiguing individuals.

Although cognitive components are generally recognized in the existing conceptualizations of cyber security fatigue, they are generally considered as a precursor to poor attitude rather than in their own right. Two factors of fatigue are likely to occur without any reference to attitudes. These are the employee's propensity for habituation and the limits imposed on decision-making by mental resources (i.e., depletion). Each supply a mechanism through which exposure to cyber security demands can result in fatigue-like behaviors but which may not coincide with a poor attitude to cyber security.

Habituation of Actions and to Advice

Employees form cyber security habits through their daily interactions with cyber security-related tasks. Cybersecurity-related stimuli can include notifications employees receive (such as an SSL warning on a website), and reminders of cyber security from other sources (e.g., educational stimuli presented as part of cyber security training, or warnings of data breaches in the media) (Ablon et al., 2016). Each of these events is stimuli to which the employee must respond (Amran et al., 2018). However, consistent with the principles

of conditioning theory, employees' appraisal of these stimuli will change. The strength of orientation toward the stimuli as well as the appraisal of threat or importance will diminish over time in a process often referred to as habituation (Herley, 2009). Such habituation is likely to relate to both advice-related stimuli as well as the requirement to respond (i.e., action-related).

The likelihood of an individual becoming habituated to stimuli depends on multiple components. The effect is likely when the stimuli are very similar or identical, appear in close succession or in a predictable fashion, and when the employee associates no immediate negative outcomes with ignoring the stimulus (Amran et al., 2018). Cybersecurity situations are often of this nature. Warnings and alerts often appear similar and occur at predictable intervals. Employees may also often receive little feedback regarding their cyber security behaviors (Shepherd et al., 2014), so that there is nothing to reorientate them toward, or reappraise, the importance of the stimuli.

Greater habituation or reduced orientation toward stimuli may also occur when understanding of the content of warnings is poor due to complex technical language (Bravo-Lillo et al., 2011). Thus, while employees may pay attention to a warning for the first few exposures, they will gradually come to dismiss it without processing the content (Anderson et al., 2015). Some researchers have suggested that this process is largely unconscious, as a habituated individual filters out information without conscious attention (Anderson et al., 2016). To demonstrate this effect, a study by Felt et al. (2012) tasked participants with installing an Android app. Fourty-two percent of individuals did not remember seeing the security permission dialog they agreed to install the app. Sotirakopoulos et al. (2011) found similar results in relation to secure socket layer (SSL) warnings.

Within the four-component model, habituation is a cognitive type of fatigue (see Table 1). It can be both action-related and advice-related, that is, it is likely that employees can filter-out cyber security advice, in the form of emails, training, or posters in the workplace, in much the same way as warnings or popups (Amran et al., 2018).

The Limits of Human Decision-Making

Multiple terms are available in literature to describe an internal state where mental performance suffers due to unavailability of mental resources (Pignatiello et al., 2020). Different disciplines refer to this state as ego depletion, self-regulatory fatigue, decision fatigue, mental fatigue, and cognitive-type fatigue (e.g., Hopstaken et al., 2015; Pignatiello et al., 2020; Vohs et al., 2008). While there are distinctions between these terms, there is a lack of consensus regarding their use (Pignatiello et al., 2020). As a result, they are often used interchangeably (Lurquin & Miyake, 2017). Overall, these terms share the common idea that the consumption of cognitive resources diminishes performance on future cognitive tasks, either due to the lack of available resources or the lack of motivation to dedicate further resources to the current task (Baumeister & Vohs, 2016).

This article uses the term depletion to reflect the commonality between these different terms: resource expenditure. When depletion occurs as a result of previously expended mental effort on a cyber security-related task, performance on future tasks suffers (Coopamootoo et al., 2017). This is not necessarily associated with an increasingly negative mood or attitude (Baumeister & Vohs, 2016), but simply because of the lack of resources to make a better decision. To use an example from a different context, a rock-climber may become tired after a few hours, but they would likely still express a positive attitude to the sport (Danziger et al., 2011). Likewise, the constant decision-making required to maintain good cyber security (e.g., creating strong passwords, checking email authenticity) can exhaust employees, without causing a poor attitude toward cyber security as a whole. Therefore, within the four-component model, depletion is an action-related, cognitive type of fatigue.

One type of depletion, Ego Depletion or Self-Regulatory Fatigue, occurs as a result of cognitively effortful acts of self-regulation. Self-regulation describes the acts of inhibition where heuristic thinking is overridden by systematic thinking (Kahneman et al., 2002). Schmeichel (2007) argue that self-regulation shares significant overlap with the concept of executive control, which refers to one's allocation of attention, maintenance of working memory, and the switching from one mental task to another. Acts of self-regulation are effortful and deplete cognitive resources (Baumeister et al., 1998). Once these resources are diminished, the individual enters a state of ego depletion, impairing future regulatory ability (Vohs & Heatherton, 2000). Cybersecurity-related examples of self-regulation include the creation of strong and unique passwords by overriding an initial impulse to create a weak password (Coopamootoo et al., 2017; Reeves et al., 2020b), and the use of systematic thinking over heuristic thinking to assess the legitimacy of a potential phishing email (Goel et al., 2017; Luo et al., 2013).

There has been a growing research interest in understanding the effects of depletion on cyber security. Groß et al. (2016) found that depletion diminishes the capacity to create strong passwords, suggesting that cognitive effort is necessary for the creation of strong passwords. Conversely, Reeves et al. (2020b) found that depletion was not associated with poorer password-creation behaviors when individuals were unaware they were being examined. This suggests password creation is largely an automatic, unconscious action for many employees. This latter study demonstrates the efficacy of the four-component model for identifying possible explanations for unexpected outcomes.

The Role of Heuristics

Dual process theory holds that people make decisions via two distinct processes: systematic and heuristic thinking (Luo et al., 2013; Wason & Evans, 1974). Systematic thinking is

effortful as it is consciously monitored and controlled (Kahneman, 2003). Conversely, heuristic thinking is automatic and less effortful (Kahneman, 2003). Heuristic decision-making tends to be faster and requires less cognitive effort, but the accuracy of the individual's decision-making suffers due to a reliance on mental shortcuts and biases (Luo et al., 2013). Conversely, systematic decision-making tends to be more accurate but is slower and requires greater cognitive effort (Luo et al., 2013). Whether people use systematic or heuristic thinking in a given decision-making instance depends on various individual and situational factors. In the case of cyber security, it is likely that heuristic decision-making is a factor preventing the adoption of best practice cyber security behaviors (Pfleeger & Caputo, 2012). For example, Goel et al. (2017) found that individuals became more susceptible to phishing attacks when the researchers manipulated the heuristic of framing. As heuristic thinking is often automatic or instinctive, the observation of heuristic thinking is not sufficient to indicate the presence of cyber security fatigue.

Individuals in depleted states described above are less able to override heuristic thinking to use systematic thinking, leading to a greater reliance on heuristic decision-making (Pocheptsova et al., 2009). Furthermore, heuristic thinking is common in a depleted state as it is less cognitively demanding, thereby requiring less of the already depleted mental resources. Therefore, among other cyber security risks, depleted individuals may be more likely to create weaker passwords and fall for phishing attacks.

Similar to ego depletion, Hopstaken et al. (2015) define mental fatigue (or cognitive fatigue) as reduced motivation for effortful activity. Similarly, decision fatigue describes the phenotypic expression of a depleted state resulting from self-regulation or other effortful tasks (Pignatiello et al., 2020). Each of these states produces similar outcomes. Like ego depletion, mental and decision fatigue relate to reductions in future task performance (Hopstaken et al., 2015), decision-making proficiency (Pignatiello et al., 2020), and a greater reliance on heuristic thinking (Pignatiello et al., 2020; Pocheptsova et al., 2009). Therefore, it is important to consider the effect that this greater reliance on heuristic thinking will have on cyber security behaviors. The remainder of this section discusses three key heuristics in relation to cyber security: anchoring, framing, and the availability heuristic.

Anchoring occurs when people base decisions or judgments on initial value or belief (Schwenk, 1984). Even when new information becomes available, decisions remain largely anchored to the original judgment. For example, software developers may only slightly alter previous code or design, even when new information demonstrates the presence of security vulnerabilities (Ceric & Holland, 2019; J. Parsons & Saunders, 2004). Epley and Gilovich (2005) suggest that this insufficient adjustment is due to the cognitive effort required to make adjustments. Therefore, we expect that individuals in a state of depletion will tend to adjust their decisions very little, thereby preserving their cognitive resources. This is problematic in contexts where the original anchor is significantly different from the optimum cyber security behavior. For example, employee-created passwords are often low in complexity and they tend to reuse them across systems (Siponen et al., 2020). These behaviors form an anchor for what the individual considers acceptable. SETA programs that aim to encourage adjustment toward more optimal work behaviors may find limited success if the employee must perform that behavior at a time when the workday has depleted them (e.g., assessing emails for veracity at the end of the workday). In a password-creation context, a depleted individual will likely not increase the strength of their passwords if advised to do so (Ceric & Holland, 2019; Reeves et al., 2020b).

Another relevant heuristic, framing effects, refer to when people make different decisions and when they perceive the decision as pursuing a gain or avoiding a loss (Tversky & Kahneman, 1981). Typically, people are more willing to choose a risky option when the situation is framed as a loss, but prefer the safer option when the same situation is framed as a gain (Highhouse & Yüce, 1996). For example, phishing emails framed to emphasize a potential monetary loss are more successful than those which emphasize a monetary gain (Goel et al., 2017). In practice, people can reduce their susceptibility to framing effects by using systematic thinking. However, this is unlikely to occur in a depleted state.

Finally, the availability heuristic is a mental shortcut used to assess the likelihood of risks occurring and their severity should they occur (Kahneman, 2003). Risks that people are able recall more easily are often considered to be more likely and severe. However, this means people often consider less salient risks to be more rare and less severe than they are in reality (Pfleeger & Caputo, 2012). As organizations are often unaware of cyber security breaches until sometime after it has occurred, it is hard to keep employees informed of the prevalence of cyber security risks. Therefore, the availability heuristic may cause employees to have a reduced perception of the likelihood and severity of cyber security risks. While this can be overcome with systematic processes, as discussed, this is unlikely when fatigued.

Overall, the literature suggests that: (a) repetitive or effortful cyber security-related behaviors can result in depletion, (b) employees are more likely to use heuristic decision-making when depleted, and (c) these heuristic decisions result in poorer cyber security behaviors.

Attitudinal-Type Fatigue

While heuristics provide an explanation for largely unconscious decision-making, it is important to understand the factors that influence employee decisions when they are able to use systematic processes. In these instances, the attitude the employee has toward cyber security is relevant. A review of the literature identifies three primary ways that we can understand how a poor attitude regarding cyber security forms: as a poor perception of cost and benefits, as a result of reactance,

or as a result of moral disengagement. This section will review each approach in turn and discuss each in relation to the four-component model of cyber security fatigue.

Poor Perception of Cost and Benefits

Employees will weigh the costs and benefits of complying with a particular security policy. The theory of reasoned action and theory of planned behavior (TRA/TPB) hold that, among other considerations, can explain how individuals use these factors to make decisions (Ajzen, 1991; Singer et al., 2014; Venkatesh et al., 2003). Davis (1989) apply this approach to a technology context. The technology acceptance model (TAM) seeks to identify the factors that motivate individuals to adopt a given technology (Davis, 1989). Although many factors have been identified, the most robust predictors of technology adoption are how easy the technology appears to be to use (perceived ease of use), and how effective the technology is at fulfilling its intended purpose (perceived usefulness) (Abdullah & Ward, 2016; Zolotov et al., 2018).

While TAM is effective at predicting technology adoption, Herath et al. (2014) question its utility in predicting cyber security-related technology adoption. According to TAM, organizations design their technology systems to be of value to individuals and increase workplace productivity (Davis, 1989; Herath et al., 2014). Thus, TAM sees technology acceptance as an act of approaching something desirable (Liang & Xue, 2009). However, in the case of adopting cyber security technology, the primary purpose of the technology is not to directly increase productivity but to avoid cyber security threats; therefore, it is an act of avoiding an undesired end-state (e.g., data loss or identify theft). Liang and Xue (2009) argue that the motivations for approaching and avoiding differ markedly and, therefore, cyber security threat avoidance behaviors cannot be fully understood by the use of an approach-based theory alone.

Consequently, Liang and Xue (2009) used coping theory, TAM, and TRA/TPB to develop technology threat avoidance theory (TTAT). Coping theory holds that avoidance of risk relates to two factors: threat appraisal and coping appraisal (Lazarus, 1966). Threat appraisal refers to the extent to which an individual believes the threat is real and applies to them, as well as the severity of the impact should the risk event occur (Liang & Xue, 2009), whereas coping appraisal refers to the individual's perception that they are able to perform actions required to avoid the threat. To use malware as an example, an individual may believe that while the threat is legitimate, they may not believe that they are able to access and understand the antivirus software that will help them avoid the threat. They may, therefore, have limited motivation to adopt such technology. In this sense, coping appraisal is conceptually similar to the primary factors of TAM: perceived ease of use and perceived usefulness (Herath et al., 2014).

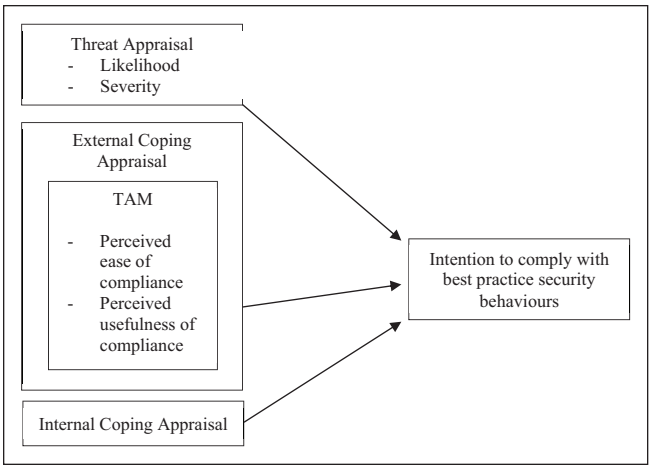

Figure 3. The expanded technology threat avoidance theory adapted from Herath et al. (2014).
Note. TAM = technology acceptance model.

However, the conceptualization of coping appraisal used in TTAT only considers one aspect of coping. External coping appraisal refers to the extent to which an individual believes they can use a piece of protective technology, whereas internal coping appraisal refers to their perceptions that they can detect and avoid the threat without the need for any external technology. Herath et al. (2014) argue that the existing TTAT considers only the external coping appraisal of individuals and, therefore, misses a key aspect of motivation. If an individual believes they are capable of avoiding cyber security threats without the use of external technology, they will likely not adopt the technology, even if they have favorable views about its ease of use, usefulness, or the severity of the threat. Herath et al.'s results supported internal coping appraisal as a significant predictor of intention to adopt security technology. Figure 3 presents the expanded-TTAT (eTTAT).

The eTTAT predicts that, when presented with a decision of whether to comply with the recommended security behaviors, an employee using systematic thinking will likely weigh the likelihood of a negative outcome (e.g., getting caught); the perceived ease of compliance; how useful their compliance will be, and, how well they are able to cope should they not comply. An individual who perceives low utility of their compliance action, low ease of compliance, and low likelihood of a poor risk outcome (e.g., getting caught or causing a breach) is likely to demonstrate fatigue-like behaviors where they disengage from cyber security demands. In effect, a poor perception of cost and benefit is an attitudinal type of fatigue and this can be either advice-related or action-related.

Reactance

While personal cost–benefit analyses likely play a role in employee decision-making, fatigued employees will often

use other, less rational, decision-making processes. One example is reactance. This refers to a negative emotional response caused by threats-to or losses-of behavioral freedom (Lowry & Moody, 2015). The behavioral consequences of reactance often involve attempts to reassert a sense of self-determination (Burgoon et al., 2002), often by rejecting authority (Lowry & Moody, 2015). Said simply, when security policies tell employees that they cannot do something, there is a chance of deliberate disobedience. Reactance is prevalent in many contexts, from adoption of health care advice (Brown et al., 2016) to climate change denial (Lu et al., 2017). In each case, reactance results from a perceived violation of control over one's own decision-making (i.e., freedom) (Brehm, 1966). When an authority figure limits the options that are available, the individual perceives disobedience as the only action that enables their own agency (Brehm & Brehm, 1981). For this reason, more stringent behavioral restrictions and monitoring in workplaces can backfire and increase pernicious employee behavior (Posey et al., 2011).

Lowry and Moody (2015) proposed a reactance model aimed at predicting compliance intention with cyber security policies (a.k.a. intent-to-comply or ITC). As expected, reactance predicted significantly lower ITC. Furthermore, state reactance (i.e., how reactant an employee felt regarding a particular cyber security policy) related to only two factors: perceived threat to freedom and trait reactance. Perceived threat to freedom refers to the employee's perception that the policy is limiting their freedom, whereas trait reactance refers to their general propensity to become reactant in any context (Dillard & Shen, 2005). Therefore, they suggest that a less stringent and restrictive cyber security policy will reduce reactance, thereby increasing compliance (Lowry & Moody, 2015). Given that reactance consists of a disobedient attitude resulting from overly restrictive recommendations at work, we consider it to be an advice-related, attitudinal type of fatigue within the four-component model.

Acknowledging reactance may present a dilemma for organizations. Although it may be true that a cyber security policy that allows greater freedom will result in greater compliance, a question remains as to whether such a policy will be effective. In other words, is 90% compliance with a more permissive policy better than 10% compliance with a stringent one? We can view the answer to this through the lens of the four-component model. Reactance is an advice-related, attitudinal type of fatigue. As a result, efforts to address reactance should also consider the potential effects on action-related, cognitive factors. While providing greater agency may likely improve employee attitude toward cyber security, it also entails greater decision-making responsibility on the part of the employee. This greater cognitive load may increase the instances of depletion and habituation, leading to similar problematic behaviors that would result from a poor attitude (Hickman et al., 2018). As an example, an employee who is newly allowed to install software on their work machine may be initially motivated to ensure the software they install is safe (i.e., reduced attitudinal-type fatigue). However, over time they will become tired of assessing all of the information available in order to determine whether the software is safe, or they may become habituated to the warning messages presented when they download and install the software (i.e., increased action fatigue). Therefore, their behavior is a risk to the organization which would not have been present had the organization not allowed employees to install software. The four-component model enables cyber security practitioners and organizations to know what factors they should consider to ensure the most desirable employee behavior for their industry, organization, or a specific situation. In this instance, the organization should assess the risk of cognitive-type fatigue resulting from efforts to reduce attitudinal-type fatigue to determine which outcome is preferable.

Moral Disengagement

The ways in which employees respond to intrusive cyber security policies will also depend on the type of coping strategy they adopt in such situations. Coping theory groups the outcomes of stress creators into two categories: emotion- and problem-focused (Perrewé & Zellars, 1999). Problem-focused coping involves direct efforts to manage or alter the stressful situation. Employees can achieve this in the workplace by eliminating obstructions that prevent them from performing tasks to a high standard or by seeking to increase their knowledge or skills. Emotion-focused coping involves changing the way one thinks or feels about the stressful situation. This process involves reappraisals and distortions of reality to make the situation seem better than it is (D'Arcy et al., 2014). In the case of cyber security, an emotion-focused response may be to categorize cyber security as unhelpful or unwarranted. In this way, individuals frame their inability to keep up with workplace cyber security demands as their own decision rather than a lack of ability (Atanasoff & Venable, 2017). D'Arcy et al. (2014) argue that employees will use emotion-focused coping in instances where no problem-focused solution is available. For example, an employee may not always have the ability to object to a new cyber security policy, in which case they will rely more heavily on emotion-focused coping.

This emotion-based coping approach can give rise to different problems. In the case of cyber security, emotion-focused coping will often result in employees no longer believing that disobeying the organization's security policy is the wrong thing to do (i.e., moral disengagement; Moore et al., 2012). In this state, the employee reduces their distress regarding their inability to comply with an overly stringent security policy by simply categorizing the policy as unimportant. Employees may come to view cyber security issues themselves as unimportant and this can result in behavior which deviates significantly from best practice (Hwang & Cha, 2018).

Moral disengagement may also occur from constant exposure to reports of data breach incidents from media and other sources. In recent years, high-profile breaches such as the Target breach (Ablon et al., 2016), Ticketmaster (Gibb, 2018), and PageUp breaches (Sam, 2018) mean that individuals see constant reports of organizations having their data lost or compromised. It is understandable, therefore, that some individuals express feelings of nihilism (Choi & Jung, 2018; Reitberger & Wetzel, 2017). Consistent with this view, Ablon et al. (2016) found that people exposed to a data breach often express the belief that data breaches are just part of modern life and not worth worrying about, even if the breach likely involved their personal data.

In addition, employees may become morally disengaged in workplace settings if they feel that, unlike at home, workplace cyber security is not their responsibility. This forms a type of moral disengagement where employees rely on security experts in their organization to protect them from cyber security threats (Blythe, 2015). Blythe and Coventry (2018) found that low perceived responsibility predicted poor employee security behavior in regard to the use of anti-malware software and security updates. Interestingly, this was not the case in relation to email-use behaviors (Blythe & Coventry, 2018). The authors suggest that this may be a result of the increased frequency of involvement with email over antivirus or software updates. Due to the frequent use of email throughout a working day, employee behavior may become more habitual (Blythe & Coventry, 2018). The results of Blythe and Coventry (2018) support the assertion of the four-component model that targeting attitudinal-type fatigue (low perceived responsibility) will not be effective if the type of the fatigue in the workforce is cognitive (habituation and depletion).

Burnout

New or confusing technology can cause stress for employees and lead to a poor attitude toward the technology (Atanasoff & Venable, 2017). Brod (1982) used the term technostress to refer to these technology-related causes of stress. D'Arcy et al. (2014) identified that three causes of technostress are relevant to cyber security: overload, complexity, and uncertainty (D'Arcy et al., 2014). The first, techno-overload, is where employees perceive that technology is adding to their workload rather than reducing it. The remaining stress creators—complexity and uncertainty—refer, respectively, to employee perceptions that new technology is far too complicated for them to understand, and that technology is changing so rapidly that they can never catch-up (Tarafdar et al., 2010). The relationship between technostress and workplace behaviors has been extensively studied (Atanasoff & Venable, 2017; Ayyagari, 2008; Tarafdar et al., 2010, 2015). Employees suffering from technostress are far less likely to adopt new technologies, are less productive, less satisfied with their job, and have greater turnover intention (Johnson & Yanson, 2015; Zolotov et al., 2018).

Left unaddressed, prolonged stress in the workplace can lead to burnout (Trépanier et al., 2015). Employees in a state of burnout often report feeling overworked and exhausted (Demerouti et al., 2001). They also appear detached and depressed and may express negative attitudes toward their work (Demerouti et al., 2010). These symptoms form two dimensions of burnout: emotional exhaustion and cynicism (Trépanier et al., 2015). Under the four-component model, burnout is relevant to both advice-related and action-related fatigue. Action-related emotional exhaustion and cynicism could manifest respectively as feelings of exhaustion when performing cyber security behaviors and questioning the feasibility of performing those behaviors. In contrast, advice-related emotional exhaustion and cynicism would respectively manifest as feeling exhausted when others raise the topic of cyber security and employees questioning the efficacy of the advice or policy (D'Arcy et al., 2014; Stanton et al., 2016). As cynicism and emotional exhaustion are largely affective states, we classify burnout as attitudinal-type fatigue within the four-component model.

While it is unlikely that cybersecurity demands in isolation would cause employee burnout, Choi & Jung (2018) have identified that employees can exhibit symptoms consistent with burnout when they must cope with stressful cybersecurity-related workplace demands. Furthermore, they found that burnout predicted intention to disclose personal information online as well as moral disengagement from online privacy issues. This is a concern for existing SETA programs, many of which aim to educate employees of the importance of maintaining cyber security (D'Arcy et al., 2009).

While burnout is an extreme example of an outcome of workplace stress, it remains an important consideration for workplace cyber security. Many employees perceive that the cyber security technological systems at their workplaces are making their lives harder (Calic et al., 2016; Stanton et al., 2016) and will, therefore, increase their technostress and risk of burnout. Any intervention aimed at tackling the issue of cyber security, either by technological or human factor methods, should consider the potential stress this may be putting on employees. A highly sophisticated technological security solution may not be worthwhile if its use results in employee technostress. Likewise, frequent training may lead to overload and, ultimately, burnout.

Research Implications

Researchers have used terms such as security fatigue, privacy fatigue, and security disengagement to refer to concepts similar to cyber security fatigue. The sections to follow will review these existing approaches through the lens of the four-component model.

Existing Attitudinal Theories

Multiple theories are available that attempt to explain employee attitudes to cyber security. Furnell and Thomson (2009) used the term security fatigue to refer to "a situation in which employees have been following good practice and then drift (or completely switch) into a mode in which they become tired or disillusioned with it" (p. 7). The authors conceptualize fatigue as a result of a cost–benefit analysis on the part of the fatigued individual. Essentially, employees weigh the difficulty of complying with cyber security demands (e.g., a particular cyber security policy) and the effort required to comply with the perceived importance of doing so. If the importance does not outweigh the costs, there is potential for the individual to become fatigued (Furnell & Thomson, 2009). While this approach addresses the attitudes of employees, here referred to as perceived cost and perceived value, it does not capture some cognitive elements of fatigue. Even if their attitude to cyber security is favorable, employees may begin to make mistakes due to depletion resulting from the often-repetitive behaviors required to maintain cyber security (see Danziger et al., 2011; Hickman et al., 2018; Stewart et al., 2012). Likewise, employees may exhibit fatigue-like behaviors as a result of an unconscious tuning-out of cyber security information. As these mechanisms do not relate directly to perceived cost or value, efforts to manipulate perceived importance will be largely ineffective at changing these behaviors (Malimage, 2013).

Similarly, Stanton et al. (2016) highlighted the relationship between fatigue and poor perceived value of cyber security. They argue that this is partly due to the lack of awareness many employees have regarding the frequency and severity of cyber security incidents. To address this, Stanton et al. (2016) suggest that organizations should make employees aware each time a cyber security event occurs. This heightened awareness should increase their appreciation of the importance of cyber security, leading to better behaviors. In the same vein, using the eTTAT, Liang and Xue (2009) suggest that employee behavior will improve when they appreciate the need for cyber security (i.e., increased threat appraisal). However, these approaches do not consider the increase to action fatigue as a result of these interventions. While it is true that updates regarding the frequency of cyber security incidents, in the form of emails or popups, would increase employees' appreciation of cyber security risks, they could also result in employees tuning-out and ignoring these notifications. For those employees who do not ignore the notifications, and instead make a conscious effort to read and understand each one, doing so will add to their workload and over time lead to depletion.

In an attempt to operationalize most existing conceptualizations of cyber security fatigue, Choi & Jung (2018) developed the Privacy Fatigue Scale. They define privacy fatigue as a "sense of weariness toward privacy issues in which individuals believe that there is no effective means of managing their personal information on the internet" (p. 44). Much like moral disengagement, the authors suggest that this occurs as a result of people being aware of frequent data breaches occurring, leading to the perception that they have no control over their personal information online. Choi & Jung (2018) used burnout as a base for their model, thus incorporating cynicism and emotional exhaustion as their two main elements. While these factors are important, this approach may not explain fatigue-like behaviors that result from an employee tuning-out cyber security information or due to nonrational processes. For example, a reactant employee may appear cynical and disengaged. If cyber security professionals misdiagnose these symptoms as signs of burnout, they may misdirect their efforts may to increasing organizational supports rather than reducing the employees' perceived threat to their freedom (Lowry & Moody, 2015).

Existing Cognitive Theories

As practitioners are understandably interested in employee compliance, it is common to see cyber security researchers using compliance-based theoretical approaches (Guzman, 2007). These approaches tend to view employees as rational actors whose compliance behavior results from a balance of intrinsic and extrinsic motivators (Hofeditz et al., 2017). In the four-component model, we consider these approaches to be attitudinal in that they largely concern the perception of the cost and benefit associated with an action, or are otherwise consciously performed. While these approaches are useful, the literature also emphasizes the importance of nonrational-actor approaches.

For example, fatigue-like behaviors can result from employees becoming habituated to all stimuli relating to cyber security (Amran et al., 2018). As this occurs unconsciously, these behaviors are not "rational" in the traditional sense, and therefore rational-actor approaches will fail to fully explain them. Researchers have suggested multiple possible interventions to avoid this occurring (Amran et al., 2018; Anderson et al., 2015; Malimage, 2013). One such approach suggests that information technology systems should present cyber security-related stimuli in varying ways to prevent habituation to similarly presented warnings, popups, and emails. Anderson et al. (2015) developed a polymorphic warning system, which changed the appearance of warnings each time they were presented to the participant. A constantly changing design forces individuals to pay more attention to warnings, but even varied stimuli can become tiresome over a full workday. The four-component model suggests that forcing cognitive attention in this way is likely to quickly deplete employees (Pignatiello et al., 2020). Moreover, this constant intrusion into the work day will increase employee workload, leading to stress and fatigue (Salvagioni et al., 2017). The irritation may also lead employees to become reactant (Lowry & Moody, 2015) and these reactant behaviors may be worse than the

Table 2. The Four-Component Model Used as a Framework for Diagnosis and Intervention Planning.

	Issue	Mistaken diagnosis	Suboptimal intervention	Recommended intervention
Mistaken source	[1]Advice-related source Employees are tired of being told what to do.	Action-related source Interacting with workplace cyber security systems is tiring.	Simplify the workplace cyber security systems with which employees interact, such as authentication systems.	Try to set up intuitive policies to minimize the needs for SETA programs and minimize the extent to which policies negatively affect employees.
	[3]Action-related source Interacting with workplace cyber security systems is tiring.	Advice-related source Employees are tired of being told what to do.	Try to set up intuitive policies to minimize the needs for SETA programs and minimize the extent to which policies negatively affect employees.	Simplify the workplace cyber security systems with which employees interact, such as authentication systems.
Mistaken type	[2]Attitudinal-type fatigue Employees do not appreciate the need for cyber security.	Cognitive-type fatigue Employees make mistakes due to mental tiredness	Align critical processes so that high-risk activities do not occur when employees are fatigued, as far as possible, and reduce the cognitive load placed on employees by workplace systems.	Implement a SETA program to increase employee appreciation of cyber security.
	[3]Cognitive-type fatigue Employees make mistakes due to mental tiredness	Attitudinal-type fatigue Employees do not appreciate the need for cyber security.	Implement a SETA program to increase employee appreciation of cyber security.	Align critical processes so that high-risk activities do not occur when employees are fatigued, as far as possible, and reduce the cognitive load placed on employees by workplace systems.

Note. [1,2,3]Respectively, case studies 1, 2, and 3 provide an illustrative example of these misdiagnoses and recommendations (p. 24). SETA = security education, training, and awareness.

behaviors the intervention was seeking to address. Therefore, while polymorphic warnings may be effective at reducing habituation, their effectiveness at improving cyber security behaviors could be limited and warrants further empirical exploration.

Applied Implications

Cybersecurity practitioners may benefit from a schematic such as that displayed in Table 2 when considering an intervention or process change. As Table 2 indicates, the first decision will be to determine the kind of fatigue that is occurring, while also being mindful of the possibility that multiple types of fatigue may be occurring at once. The model would then encourage the practitioner to consider the factors that are contributing to the identified type of disengagement (e.g., reactance, habituation), and a schematic such as that displayed in Table 1 may assist. For example, an organization might observe that employees are consistently falling for phishing emails. The temptation here may be to attempt to educate these employees on skills to detect a phishing email as well as the overall benefits of cyber security. However, the four-component model would encourage caution. It may be that employees already know how to identify phishing emails, but they are simply fatigued from the sheer number of emails they encounter each day.

Another possibility is that employees may be already overloaded with cyber security information and advice, which they perceive to change frequently and be far too complex (Stanton et al., 2016). As a result, providing further awareness training will likely add to this overload and unlikely to encourage greater compliance. In addition, it may be that the employees are simply habituated to their environment. Awareness programs in this context may not be effective if the employees are unconsciously tuning-out cyber security-related stimuli and advice. A temptation in this context may be to change the design of the relevant cyber security systems or warnings to interrupt the habituation (Brustoloni & Villamarn-Salom, 2007). However, it is likely this increased decision-making load on the employee will itself be fatiguing (Pocheptsova et al., 2009).

A question arises from the four-component model as to whether it is possible to combat fatigue completely. It seems that any intervention that addresses one aspect of fatigue will likely result in other kinds of fatigue. Thus, are there interventions that can succeed in avoiding cognitive

limitations and improving attitude, both in relation to advice and action? In some cases, such interventions will be possible, but often this will not be the case. An important applied feature of the four-component model from an organizational perspective is that it provides a guide for what approach an organization should take based on the type of fatigue they observe, that is, while the behavioral outcomes of these two states will be similar, the causes will be different. Accordingly, when comparing employee behavior to best-practice, it may be possible for researchers to inform industry as to which kind of fatigue poses least risk for each context when no intervention that addresses all dimensions is available (e.g., IT industry vs. finance, or email-use behaviors vs. password management).

For this reason, before an organization implements a new cyber security process, they should consider several questions. For example, will employees perceive the new process to be restricting their freedom? Will it add to their workload? Will it be problematic if employees begin to tune-out this system or process, and is this likely to occur? If any of these are likely, then the practitioner should consider how they will manage these behaviors, and what the organization can do to minimize the level of reactance, habituation, or other disengagement that may result from the change. In the likely case that no perfect solution is available, which succeeds in minimizing both attitudinal and cognitive aspects of fatigue, the four-component model suggests pathways through which practitioners can manipulate employee disengagement and optimize employee behavior. That is, for example, sometimes a habituated employee is preferable to a reactant one, a nuance that existing approaches may overlook.

In many instances, a mistaken appraisal will not result in an intervention that is altogether detrimental. For example, if cyber security practitioners misidentify action fatigue as advice fatigue, an intervention may seek to streamline cybersecurity policies and thereby avoid the need for SETA programs. Such an intervention may also have some impact on action fatigue. Therefore, Table 2 refers to these interventions as suboptimal. While these interventions hold some value, cyber security practitioners can use the four-component model to identify an intervention that may add greater value. In the above example, a more valuable intervention may be to simplify the workplace cyber security systems with which employees interact, such as authentication systems. Likewise, an intervention that targets cognitive-type fatigue, such as by moving business critical actions away from times of the day where employees are likely to be tired, will be valuable in almost any context. However, our model holds that this is not the optimal solution to the problem of attitudinal-type fatigue, as this fatigue relates to a pervasively poor affectivity toward cyber security. The case studies to follow expand on these applications of the four-component model to different organizational settings.

Illustrative Case Studies

The following illustrative case studies demonstrate what an organization may do should they incorrectly diagnose the cause for the lack of engagement with the organization's cyber security policies. They present examples of how organizations can apply the four-component model in practice to avoid a suboptimal intervention that may exacerbate the problem. We adapted these examples from situations described by employees from various organizations as part of interviews conducted by Reeves et al. (2020a). The purpose of these case studies is not to be evidence for the four-component model, but rather as illustrations of how the model can be applied. For each scenario, we provide a description of the organizational setting, the main sources of threat and the projected outcomes before analyzing how the situation might be enhanced by applying the four-component model. Names have been changed for privacy.

Case Study 1

Miranda is an employee of a small–medium sized technology company who was interviewed as part of Reeves et al. (2020a). When interviewed about her experiences at work, she reported a preference for working independently and management permission to do so. When asked about her organization's attitude to cyber security, she described her security department as "retentive" and "over the top." She also described the organizational security policy which allows security personnel to audit personally owned devices if these devices are present in a work environment. This includes smartphones and laptops. She viewed this policy as "silly" and she saw the associated cyber security risks as "far-fetched." As a result, she described her cyber security department as "obsessed" and believed they should "calm down just a touch." She later described that she willingly breaks the organization's cyber security policy in an unrelated context as she had limited respect for the authority of the cyber security department.

From the perspective of the four-component model, we categorize Miranda's disengagement from cyber security best-practice behaviors as an advice-related, attitudinal-type fatigue. Her cyber security fatigue is advice-related as her organization's cyber security policies relating to appropriate use of technology have led her to express fatigue and disengagement. It is also attitudinal as she holds an unfavorable attitude toward the cyber security department, which appears to be less related to a transient internal state at any particular time, such as cognitive depletion, and more related to an overall affectivity she has toward her cyber security department and cyber security issues more broadly. In particular, she appears to be reactant and uninterested in the benefits of cyber security. However, while it appears that Miranda's fatigue is largely advice-related, her description of "obsessive" security

department requirements may indicate that there is also an action-related component. Therefore, in this situation, it would be worth further exploring the source of her fatigue in interview or via standardized testing.

Miranda's situation demonstrates how easy it might be to misdiagnose an employee as solely experiencing action-related fatigue and miss the advice-related component. This misperception could encourage unnecessary simplification of cyber security systems or the allocation of additional resources to greater training (Pham et al., 2019). As this approach does little to change the perception of the policy as a restriction on the employee's freedom, this will have little effect.

Case Study 2

Brian is a former employee of a small–medium sized organization in the service industry. He was interviewed as part of Reeves et al. (2020a) on his experience as the manager in charge the cyber security of the organization's operations. On the topic of his experiences with cyber security training videos, he expressed that the training content that was available at his previous employer was substandard. He described receiving the training as "terrible, really just horrible" and said he needed "a red-hot poker to open up my eyes, it's so boring." He also advised that the delivery of the training was ineffective, as he felt that "the sponge is full, I'm not interested. I've been doing this all day and I am absolutely sick of it." He attributed the poor quality of the training to the upper management, who he believed had a "care factor of 0" and an attitude of "you have to do this, [but] we're not going to give you any money to do it." He also described an apparent disconnect between the management's lack of concern internally regarding cyber security and their external communications when cyber security incidents occur. Specifically, he described a situation where a cyber security incident occurred, and the management response was "it's all tears! And oh we apologise! [. . .] they're all like we're very sorry, we're very sorry! But the damage has been done, you can't put the genie back in the bottle." These descriptions indicate that Brian was experiencing emotional exhaustion and cynicism regarding the cyber security approach of the organization (Choi & Jung, 2018).

Based on the four-component model, we categorize Brian's disengagement from cyber security best-practice behaviors as attitudinal-type fatigue. Specifically, his emotional exhaustion and cynicism suggest he is experiencing signs of burnout regarding cyber security. As it is common for employee burnout to be the result of overwhelming workplace demands (i.e., action-related fatigue), it may be easy to misdiagnose Brian's disengagement as a result of overwhelming cyber security-related workplace demands. However, the four-component model stresses the importance of considering both action and advice-related sources of fatigue. Brian's disengagement from cyber security best-practice behavior is better described as advice-related. This is because his emotional exhaustion and cynicism stem from overexposure to poor quality cyber security training and not an overexposure to cyber security-related workplace demands. As with Case Study 1, Brian's situation demonstrates how a misdiagnosis of the cause of employee cyber security fatigue can unintentionally exacerbate the problem. A misdiagnosis of action-related burnout in Brian's situation may encourage the allocation of resources to simplify the organization's cyber security systems. As this does little to improve the quality of the available workplace cyber security training, this will have little effect on improving Brian's attitude to cyber security.

Case Study 3

Roger is a government employee who was interviewed as part of Reeves et al. (2020a). At multiple points in the interview, he reported that he finds the information technology systems at his work frustrating to use. Specifically, he said the systems "don't talk to each other" and often take a long time to update when he changes his password. He described a common experience where a password update on one system fails to automatically update on other systems. This means he is often unsure which password he should be using. He described using this system as "painful." Due to this system, he readily acknowledged that he writes down his passwords on paper. He also indicated that he was aware that this is against the security policy. Despite breaking the policy, he advises that he appreciates the need for cyber security, but "doesn't see how else you could do it."

Within the four-component model, we categorize Roger's frustration as action-related fatigue. Furthermore, his fatigue is cognitive-type as he does not have a negative affect toward cyber security. As with the previous case studies, a misdiagnosis of his situation as attitudinal-type fatigue may result in a misdirection of resources toward a SETA program. This will be largely ineffective as it does not address the cause of his fatigue. Furthermore, subjecting Roger to a SETA program may prompt a reactant response. Instead, the simplification of the security systems is appropriate in this context.

Conclusion

The four-component model is a comprehensive way of understanding cyber security fatigue. The two categories: fatigue source (action or advice) and fatigue type (attitudinal and cognitive) encompass a number of underlying factors, as discussed throughout the article. When employees disengage from cyber security, practitioners should determine whether it is the advice or the action of cyber security that has tired the employees and then whether the disengagement is attitudinal, cognitive, or a combination of both. Conceptualizing cyber security fatigue in this way enables practitioners and management to more comprehensively and accurately understand the causes of employee cyber security fatigue and

identify the potential mitigation strategies most suitable to employees as well as their organization, situation, and risk. Furthermore, the model enables researchers to further understand the nuances of cyber security fatigue, and work toward theoretical and empirical explorations of effective interventions to address them. From a theoretical standpoint, this approach can enable a thorough empirical study of the principal dimensions and the associated factors, examining the extent to which they interact or differ depending on industry or role. From an applied standpoint, the model provides practitioners with a set of important practical considerations to guide their decision-making regarding the appropriateness and the implementation of cyber security interventions. Importantly, it solidifies the notion that a single approach is often not sufficient, and that one intervention can lead to unexpected outcomes. The four-component model provides a new theoretical conceptualization with a focus on the central goal of achieving the most appropriate applied organizational cyber security outcomes.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

A. Reeves https://orcid.org/0000-0001-6896-607X
P. Delfabbro https://orcid.org/0000-0002-0466-5611

References

Abdullah, F., & Ward, R. (2016). Developing a General Extended Technology Acceptance Model for E-Learning (GETAMEL) by analysing commonly used external factors. *Computers in Human Behavior*, *56*, 238–256. https://doi.org/10.1016/j.chb.2015.11.036

Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). *Consumer attitudes toward data breach notifications and loss of personal information*. RAND Corporation.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Amran, A., Zaaba, Z. F., & Mahinderjit Singh, M. K. (2018). Habituation effects in computer security warning. In *Information security journal: A global perspective* (Vol. 27, pp. 119–131). Taylor & Francis.

Anderson, B. B., Jenkins, J. L., Vance, A., Kirwan, C. B., & Eargle, D. (2016). Your memory is working against you: How eye tracking and memory explain habituation to security warnings. *Decision Support Systems*, *92*, 3–13. https://doi.org/10.1016/j.dss.2016.09.010

Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015, Apirl). *How polymorphic warnings reduce habituation in the brain: Insights from an fMRI Study* [Paper presentation]. The Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea.

Atanasoff, L., & Venable, M. A. (2017). Technostress: Implications for adults in the workforce. *The Career Development Quarterly*, *65*(4), 326–338.

Ayyagari, R. (2008). What and why of technostress: Technology antecedents and implications. *Dissertation Abstracts International Section A: Humanities and Social Sciences*, *68*(11-A), 4762.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. https://www.semanticscholar.org/paper/Cyber-Security-Awareness-Campaigns%3A-Why-do-they-to-Bada-Sasse/640dcc2b0958c0fc5f56772571ea52727b07c685

Baumeister, R. F., Bratslavsky, E., Muraven, M., & Tice, D. M. (1998). Ego depletion: Is the active self a limited resource? *Journal of Personality and Social Psychology*, *74*(5), 1252–1265. https://doi.org/10.1037/0022-3514.74.5.1252

Baumeister, R. F., & Vohs, K. D. (2016). Chapter two—Strength model of self-regulation as limited resource: Assessment, controversies, update. In J. M. Olson & M. P. Zanna (Eds.), *Advances in experimental social psychology* (Vol. 54, pp. 67–127): Academic Press.

Blythe, J. M. (2015). *Information security in the workplace: A mixed-methods approach to understanding and improving security behaviours* [Master's thesis]. Northumbria University. Newcastle. http://nrl.northumbria.ac.uk/30328/

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Bravo-Lillo, C., Cranor, L. F., Downs, J. S., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, *9*(2), 18–26. https://doi.org/10.1109/MSP.2010.198

Brehm, J. (1966). *A theory of psychological reactance*. Academic Press.

Brehm, J., & Brehm, S. (1981). *Psychological reactance: A theory of freedom and control.* Academic Press.

Brod, C. (1982). Managing technostress: Optimizing the use of computer technology. *Personnel Journal*, *61*(10), 753–757.

Brown, M. J., Serovich, J. M., Kimberly, J. A., & Hu, J. (2016). Psychological reactance and HIV-related stigma among women living with HIV. *AIDS Care*, *28*, 745–746. https://doi.org/10.1080/09540121.2016.1147015

Brustoloni, C., & Villamarn-Salom, R. (2007). *Improving security decisions with polymorphic and audited dialogs* [Paper presentation]. The Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, United States.

Burgoon, M., Alvaro, E., Grandpre, J., & Vouludakis, M. (2002). Revisiting the theory of psychological reactance. In J. P. Dillard & M. Pfau (Eds.), *The persuasion handbook* (pp. 213–232). https://doi.org/10.4135/9781412976046

Calic, D., Pattinson, M., Parsons, K., Butavicius, M., & McCormac, A. (2016, July). *Naïve and accidental behaviours that compromise information security: What the experts think* [Paper presentation]. The Tenth International Symposium on Human Aspects of Information Security & Assurance.

Ceric, A., & Holland, P. (2019). The role of cognitive biases in anticipating and responding to cyberattacks. *Information Technology & People*, *32*(1), 171–188. http://dx.doi.org/10.1108/ITP-11-2017-0390

Choi, H., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Coopamootoo, K. P. L., Groß, T., & Pratama, M. F. R. (2017, October). *An empirical investigation of security fatigue: The case of password choice after solving a CAPTCHA* [Paper presentation]. The LASER 2017, Arlington, VA, United States. https://www.usenix.org/sites/default/files/laser2017_full_proceedings.pdf#page=47

Coventry, L., Briggs, L., Blythe, J. M., & Tran, M. (2014). *Using behavioural insights to improve the public' s use of cyber security best practices*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

Dang, J. (2018). An updated meta-analysis of the ego depletion effect. *Psychological Research*, *82*(4), 645–651. https://doi.org/10.1007/s00426-017-0862-x

Danziger, S., Levav, J., & Avnaim-Pesso, L. (2011). Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences*, *108*(17), 6889–6892. https://doi.org/10.1073/pnas.1018033108

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. http://www.jstor.org/stable/23015462

Das, S., Wang, B., Kim, A., & Camp, L. J. (2020, January). *MFA is a necessary chore!: Exploring user mental models of multi-factor authentication technologies* [Paper presentation]. The Proceedings of the 53rd Hawaii International Conference on System Sciences, Hawaii, USA.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The job demands-resources model of burnout. *Journal of Applied Psychology*, *86*(3), 499–512.

Demerouti, E., Mostert, K., & Bakker, A. B. (2010). Burnout and work engagement: A thorough investigation of the independency of both constructs. *Journal of Occupational Health Psychology*, *15*(3), 209–222. https://doi.org/10.1037/a0019408

Denise, M. R., Rob, B. B., & David, D. (2012). *Systematic review and evidence synthesis as a practice and scholarship tool*. Oxford University Press.

Dillard, J. P., & Shen, L. (2005). On the nature of reactance and its role in persuasive health communication. *Communication Monographs*, *72*(2), 144–168. https://doi.org/10.1080/03637750500111815

Epley, N., & Gilovich, T. (2005). When effortful thinking influences judgmental anchoring: Differential effects of forewarning and incentives on self-generated and externally provided anchors. *Journal of Behavioral Decision Making*, *18*(3), 199–212. https://doi.org/10.1002/bdm.495

Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). *Android permissions: User attention, comprehension, and behavior*. https://dl.acm.org/doi/10.1145/2335356.2335360

Financial Services Information Sharing and Analysis Center. (2018). *FS-ISAC Unveils 2018 cybersecurity trends according to top financial CISOs* [Press release]. https://www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos

Furnell, S., & Thomson, K.-L. (2009). Recognising and addressing "security fatigue." *Computer Fraud & Security*, *2009*(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

Gibb, F. (2018, November). Ticketmaster faces fine over data breach that may affect millions. *News 9*.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44.

Groß, T., Coopamootoo, K. P. L., & Al-Jabri, A. (2016, May). *Effect of cognitive depletion on password choice* [Paper presentation]. The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2016), San Jose, CA, United States. https://www.usenix.org/conference/laser2016/program/presentation/gross

Groß, T., Coopamootoo, K. P. L., & Al-Jabri, A. (2019). *Effect of cognitive depletion on password choice extended technical report*. https://www.ncl.ac.uk/media/wwwnclacuk/schoolofcomputingscience/files/trs/1496.pdf

Guzman, I. R. (2007). Strategies for managing IS/IT personnel. *Human Resource Management*, *46*(3), 455–458. https://doi.org/10.1002/hrm.20174

Hagger, M. S., Wood, C., Stiff, C., & Chatzisarantis, N. L. D. (2010). Ego depletion and the strength model of self-control: A meta-analysis. *Psychological Bulletin*, *136*(4), 495–525. https://doi.org/10.1037/a0019486

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61–84. https://doi.org/https://doi.org/10.1111/j.1365-2575.2012.00420.x

Herley, C. (2009, September). *So long, and no thanks for the externalities: The rational rejection of security advice by users* [Paper presentation]. The Proceedings of the 2009 Workshop on New Security Paradigms Workshop, Oxford, UK.

Hickman, R. L., Pignatiello, G. A., & Tahir, S. (2018). Evaluation of the decisional fatigue scale among surrogate decision makers of the critically ill. *Western Journal of Nursing Research*, *40*(2), 191–208. https://doi.org/10.1177/0193945917723828

Highhouse, S., & Yüce, P. (1996). Perspectives, perceptions, and risk-taking behavior. *Organizational Behavior and Human Decision Processes*, *65*(2), 159–167.

Hofeditz, M., Nienaber, A.-M., Dysvik, A., & Schewe, G. (2017). "Want to" versus "have to": Intrinsic and extrinsic motivators as predictors of compliance behavior intention. *Human Resource Management*, *56*(1), 25–49. https://doi.org/10.1002/hrm.21774

Hopstaken, J. F., Van Der Linden, D., Bakker, A. B., & Kompier, M. A. (2015). A multifaceted investigation of the link between

mental fatigue and task disengagement. *Psychophysiology*, *52*(3), 305–315.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282–293. https://doi.org/10.1016/j.chb.2017.12.022

Johnson, R., & Yanson, R. (2015). Job satisfaction and turnover intentions during technology transition: The role of user involvement, core self-evaluations, and computer self-efficacy. *Information Resources Management Journal*, *28*(4), 38–51. https://doi.org/10.4018/IRMJ.2015100103

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *The American Psychologist*, *58*(9), 697–720. https://doi.org/10.1037/0003-066X.58.9.697

Kahneman, D., Gilovich, T., & Griffin, D. (2002). *Heuristics and biases: The psychology of intuitive judgment*. Cambridge University Press.

Kroenung, J., & Eckhardt, A. (2015). The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude-behavior relationship. *Information & Management*, *52*(6), 611–627.

Lazarus, R. (1966). *Psychological stress and the coping process* (Vol. 83). McGraw-Hill.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90. https://doi.org/10.2307/20650279

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433–463. https://doi.org/10.1111/isj.12043

Lu, H., McComas, K. A., & Besley, J. C. (2017). Messages promoting genetic modification of crops in the context of climate change: Evidence for psychological reactance, *Appetite*, *108*, 104–116. https://doi.org/10.1016/j.appet.2016.09.026

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28–38.

Lurquin, J. H., & Miyake, A. (2017). Challenges to ego-depletion research go beyond the replication crisis: A need for tackling the conceptual crisis. *Frontiers in Psychology*, *8*, Article 568. https://doi.org/10.3389/fpsyg.2017.00568

Madden, A., Bailey, C., Alfes, K., & Fletcher, L. (2018). Using narrative evidence synthesis in HRM research: An overview of the method, its application, and the lessons learned. *Human Resource Management*, *57*(2), 641–657. https://doi.org/10.1002/hrm.21858

Malimage, K. (2013). *The role of habit in information security behaviors*. (Doctoral dissertation). Mississippi State University.

Moore, C., Detert, J., Klebe Trevino, L., Baker, V., & Mayer, D. (2012). Why employees do bad things: Moral disengagement and unethical organizational behavior. *Personnel Psychology*, *65*, 1–48.

Ormond, D., Warkentin, M., & Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems*, *20*(12), 1794–1843. http://dx.doi.org/10.17705/1jais.00586

Parsons, J., & Saunders, C. (2004). Cognitive heuristics in software engineering applying and extending anchoring and adjustment to artifact reuse. *IEEE Transactions on Software Engineering*, *30*(12), 873–888.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. *Security and Privacy Protection in Information Processing Systems–IFIP Advances in Information and Communication Technology*, *405*, 366–378.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016a). *The information security awareness of bank employees*. Human Aspects of Information Security & Assurance.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016b, July). The information security awareness of bank employees. In N. Clarke & S. Furnell (Eds.), International Conference on Human Aspects of Information Security & Assurance.

Perrewé, P. L., & Zellars, K. L. (1999). An examination of attributions and emotions in the transactional approach to the organizational stress process. *Journal of Organizational Behavior*, *20*(5), 739–752. https://doi.org/10.1002/(SICI)1099-1379(199909)20:5<739::AID-JOB1949>3.0.CO;2-C

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

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

Pignatiello, G. A., Martin, R. J., & Hickman, R. L. (2020). Decision fatigue: A conceptual analysis. *Journal of Health Psychology*, *25*(1), 123–135. https://doi.org/10.1177/1359105318763510

Pocheptsova, A., Amir, O., Dhar, R., & Baumeister, R. F. (2009). Deciding without resources: Resource depletion and choice in context. *Journal of Marketing Research*, *46*(3), 344–355. https://doi.org/10.1509/jmkr.46.3.344

Posey, C., Bennett, B., Roberts, T., & Lowry, P. (2011). *When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse*. https://www.semanticscholar.org/paper/When-Computer-Monitoring-Backfires%3A-Invasion-of-and-Posey-Bennett/68f885ee5766a88717f7246c878fe8b63c0c9e91

Reeves, A., Calic, D., & Delfabbro, P. (2020a). *"Get a red hot poker and open up my eyes, it's so boring": Employee perceptions of cyber security training*. *Computers & Security* [in press].

Reeves, A., Calic, D., & Delfabbro, P. (2020b, May). *Sleeping with the enemy: Does depletion cause fatigue with cybersecurity?* [Paper presentation]. The Human Computer Interaction International (HCII2020), Copenhagen, Denmark.

Reeves, A., Parsons, K., & Calic, D. (2020, May). *Whose risk is it anyway: How do risk perception and organisational commitment affect employee information security awareness?* [Paper presentation]. The 22nd International Conference on Human-Computer Interaction (HCII 2020), Copenhagen, Denmark.

Reitberger, G., & Wetzel, S. (2017). Investigating the impact of media coverage on data breach fatigue.

Salvagioni, D., Melanda, F., Mesas, A., González, A., Gabani, F., & Andrade, S. (2017). Physical, psychological and occupational consequences of job burnout: A systematic review of prospective studies. *PLoS ONE*, *12*(10), e0185781. https://doi.org/10.1371/journal.pone.0185781

Sam, B.-J. (2018, June). PageUp breach "may have hit thousands of Aussies." *The Nation 6*.

Schmeichel, B. J. (2007). Attention control, memory updating, and emotion regulation temporarily reduce the capacity for executive control. *Journal of Experimental Psychology: General*, *136*(2), 241–255.

Schwenk, C. R. (1984). Cognitive simplification processes in strategic decision-making. *Strategic Management Journal*, *5*(2), 111–128.

Shepherd, L., Archibald, J., & Ferguson, R. I. (2014). Reducing risky security behaviours: Utilising affective feedback to educate users. *Future Internet*, *6*(4), 760–772. https://doi.org/10.3390/fi6040760

Singer, E., Couper, M. P., Fagerlin, A., Fowler, F. J., Levin, C. A., Ubel, P. A., . . . Zikmund-Fisher, B. J. (2014). The role of perceived benefits and costs in patients' medical decisions. *Health Expectations: An International Journal of Public Participation in Health Care and Health Policy*, *17*(1), 4–14. https://doi.org/10.1111/j.1369-7625.2011.00739.x

Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers & Security*, *88*, 101617. https://doi.org/10.1016/j.cose.2019.101617

Sotirakopoulos, A., Hawkey, K., & Beznosov, K. (2011, July). *On the challenges in usable security lab studies: Lessons learned from replicating a study on SSL warnings* [Paper presentation] The SOUPS, Pittsburgh, PA.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional*, *18*(5), 26–32. https://doi.org/10.1109/MITP.2016.84

Stewart, A., Ferriero, D., Josephson, A., Lowenstein, D., Messing, R., Oksenberg, J., . . . Hauser, S. (2012). `hting decision fatigue. *Annals of Neurology*, *71*(1), A5–A15. https://doi.org/https://doi.org/10.1002/ana.23531

Tarafdar, M., Pullins, E. B., & Ragu-Nathan, T. (2015). Technostress: Negative effect on performance and possible mitigations. *Information Systems Journal*, *25*(2), 103–132.

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems*, *27*(3), 303–334.

Telstra Corporation. (2018). *Telstra Security Report 2018*. https://insight.telstra.com.au/content/dam/insight/pdfs/Telstra_Security_Report_2018_PDF_FINAL.PDF

Trépanier, S.-G., Fernet, C., & Austin, S. (2015). A longitudinal investigation of workplace bullying, basic need satisfaction, and employee functioning. *Journal of Occupational Health Psychology*, *20*(1), 105–116. https://doi.org/10.1037/a0037726

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453–458. http://www.jstor.org/stable/1685855

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Vohs, K. D., Baumeister, R. F., Schmeichel, B. J., Twenge, J. M., Nelson, N. M., & Tice, D. M. (2008). Making choices impairs subsequent self-control: A limited-resource account of decision making, self-regulation, and active initiative. *Journal of Personality and Social Psychology*, *94*(5), 883–898. https://doi.org/10.1037/0022-3514.94.5.883

Vohs, K. D., & Heatherton, T. F. (2000). Self-regulatory failure: A resource-depletion approach. *Psychological Science*, *11*(3), 249–254. https://doi.org/10.1111/1467-9280.00250

Wason, P. C., & Evans, J. S. B. T. (1974). Dual processes in reasoning? *Cognition*, *3*(2), 141–154. https://doi.org/10.1016/0010-0277(74)90017-1

Zolotov, M., Oliveira, T., & Casteleyn, S. (2018). E-participation adoption models research in the last 17 years: A weight and meta-analytical review. *Computers in Human Behavior*, *81*, 350–365. https://doi.org/10.1016/j.chb.2017.12.031