Received 16 June 2022
Revised 28 November 2022
Accepted 19 January 2023

Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research

Tripti Singh
Michigan Technological University, Houghton, Michigan, USA
Allen C. Johnston
The University of Alabama, Tuscaloosa, Alabama, USA
John D'Arcy
University of Delaware, Newark, Delaware, USA, and
Peter D. Harms
The University of Alabama, Tuscaloosa, Alabama, USA

Abstract

Purpose – The impact of stress on personal and work-related outcomes has been studied in the information systems (IS) literature across several professions. However, the cybersecurity profession has received little attention despite numerous reports suggesting stress is a leading cause of various adverse professional outcomes. Cybersecurity professionals work in a constantly changing adversarial threat landscape, are focused on enforcement rather than compliance, and are required to adhere to ever-changing industry mandates – a work environment that is stressful and has been likened to a war zone. Hence, this literature review aims to reveal gaps and trends in the current extant general workplace and IS-specific stress literature and illuminate potentially fruitful paths for future research focused on stress among cybersecurity professionals.

Design/methodology/approach – Using the systematic literature review process (Okoli and Schabram, 2010), the authors examined the current IS research that studies stress in organizations. A disciplinary corpus was generated from IS journals and conferences encompassing 30 years. The authors analyzed 293 articles from 21 journals and six conferences to retain 77 articles and four conference proceedings for literature review.

Findings – The findings reveal four key research opportunities. First, the demands experienced by cybersecurity professionals are distinct from the demands experienced by regular information technology (IT) professionals. Second, it is crucial to identify the appraisal process that cybersecurity professionals follow in assessing security demands. Third, there are many stress responses from cybersecurity professionals, not just negative responses. Fourth, future research should focus on stress-related outcomes such as employee productivity, job satisfaction, job turnover, etc., and not only security compliance among cybersecurity professionals.

Originality/value – This study is the first to provide a systematic synthesis of the IS stress literature to reveal gaps, trends and opportunities for future research focused on stress among cybersecurity professionals. The study presents several novel trends and research opportunities. It contends that the demands experienced by cybersecurity professionals are distinct from those experienced by regular IT professionals and scholars should seek to identify the key characteristics of these demands that influence their appraisal process. Also,

The authors would like to acknowledge the editor of the journal and the anonymous reviewers for their valuable comments and suggestions for improving the quality of the study.

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 3 No. 2, 2023
pp. 100-126
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-06-2022-0012

there are many stress responses, not just negative responses, deserving increased attention and future research should focus on unexplored stress-related outcomes for cybersecurity professionals.

Keywords Cybersecurity, Information security, Stress, Challenge stress, Hindrance stress, Security-related stress, Coping, Savoring, Stress appraisal

Paper type Literature review

1. Introduction

Among today's most critical challenges facing modern, hyper-connected organizations is the lack of qualified cybersecurity professionals needed to support their organizations' cyber programs. In a recent survey of 1,500 global cybersecurity professionals, 59% of respondents mentioned that their organizations were at a moderate to extreme risk of cybersecurity incidents because of a shortage of cybersecurity staff ((ISC)^2, 2018). The existing cybersecurity workforce gap is estimated to be as high as 3.4 million globally (HBR, 2019). This is a pervasive problem across all industries, and the shortage has been ranked as the number one concern among industry executives, outranking budget, work-life balance and time constraints as having one of the highest adverse effects on job satisfaction among cybersecurity staff ((ISC)^2, 2018).

An increased focus on cybersecurity across both public and private organizations worldwide and a constantly evolving cyber threat landscape have increased the demand of cybersecurity professionals and simultaneously widened the gap between the lack of qualified professionals and available jobs (Vogel, 2016). In addition, the current skills gap has been exacerbated by the difficulty in retaining qualified cybersecurity professionals because the increase in ransomware and other forms of cyberattacks have subsequently increased stress to an unmanageable level, leaving cybersecurity professionals contemplating their future in the industry (Ishmael and Halawi, 2022; IBM, 2022). For example, a recent study by The International Business Machines Corporation (IBM) found that the increased number and severity of ransomware attacks have exacerbated already high stress levels among cybersecurity professionals (IBM, 2022). Cyberattacks require immediate and thorough responses from cybersecurity professionals. The first three days of responding to a cyberattack are typically the most stressful, with cybersecurity professionals often working more than 12 h per day.

Moreover, beyond the technical aspects of responding to the threat itself, cybersecurity professionals report that managing stakeholder expectations and the sense of responsibility towards their clients and team is frequently the most stressful aspect of their jobs (IBM, 2022). Further, a study by Deep Instinct (2022) suggests that managing a remote workforce, the rapid pace of digital transformation, a lack of qualified staff, longer work hours, the impossibility of stopping every threat and an expectation to be on call are some factors attributing to the high level of stress among existing cybersecurity workforce. Given the complexity and urgency of this problem, it is imperative to establish a dialog between academics and practitioners on how to best recruit and retain qualified cybersecurity professionals while recognizing the underlying condition of stress and its impact on cybersecurity professionals.

Within the information systems (IS) literature, stress has been conceptualized, defined and operationalized in numerous ways. Online Appendix 1 summarizes the extant definitions of stress and related concepts as they appear in our review of IS literature. This literature indicates that the use of information technology (IT), adherence to organizational information security (InfoSec) policies, and IS-related job characteristics are significant sources of stress among IS/IT professionals (Ahuja *et al.*, 2007; Ayyagari *et al.*, 2011; Chilton *et al.*, 2005; D'Arcy *et al.*, 2014, 2018; Galluch *et al.*, 2015; Pirkkalainen *et al.*, 2019; Ragu-Nathan *et al.*, 2008; Tams *et al.*, 2020; Tarafdar *et al.*, 2007, 2010; Windeler *et al.*, 2017; Tarafdar *et al.*, 2015; Trang

and Nastjuk, 2021; Aggarwal and Dhurkari, 2023). However, there is a distinct class of IS/IT professionals that has not been given much attention by IS scholars who have studied stress, even though it has been well-documented that they are particularly likely to experience stress in their jobs: cybersecurity professionals (Oltsik, 2019; Oltsik and Alexander, 2018; Wolff, 2019).

Cybersecurity professionals face unique stress inducing challenges in that they must manage and respond to threats in a constantly changing adversarial environment (Oltsik and Alexander, 2018) that has been likened to a war zone (Brody, 2019; Harms *et al.*, 2013). Cybersecurity professionals are often the first responders to cyber events, such as breaches or alerts of suspicious activity within their firms. They must maintain a vigilance that is often unmatched among other organizational employees. Further, cybersecurity professionals frequently report feeling underappreciated for their efforts in this regard (Louie, 2018). Cybersecurity professionals report that communication problems with management (Louie, 2018), high workload, challenges with the ever-changing nature of technology and organizational technology initiatives (e.g. moving applications to the cloud, deploying IoT, etc.), and a frequent lack of security oversight for new IS projects (Oltsik, 2019) all contribute to a high level of stress in their profession. Under such stressful conditions, cybersecurity professionals have been shown to exhibit poor security-related decision quality, narrower attention and poorer working memory (Anderson *et al.*, 2016).

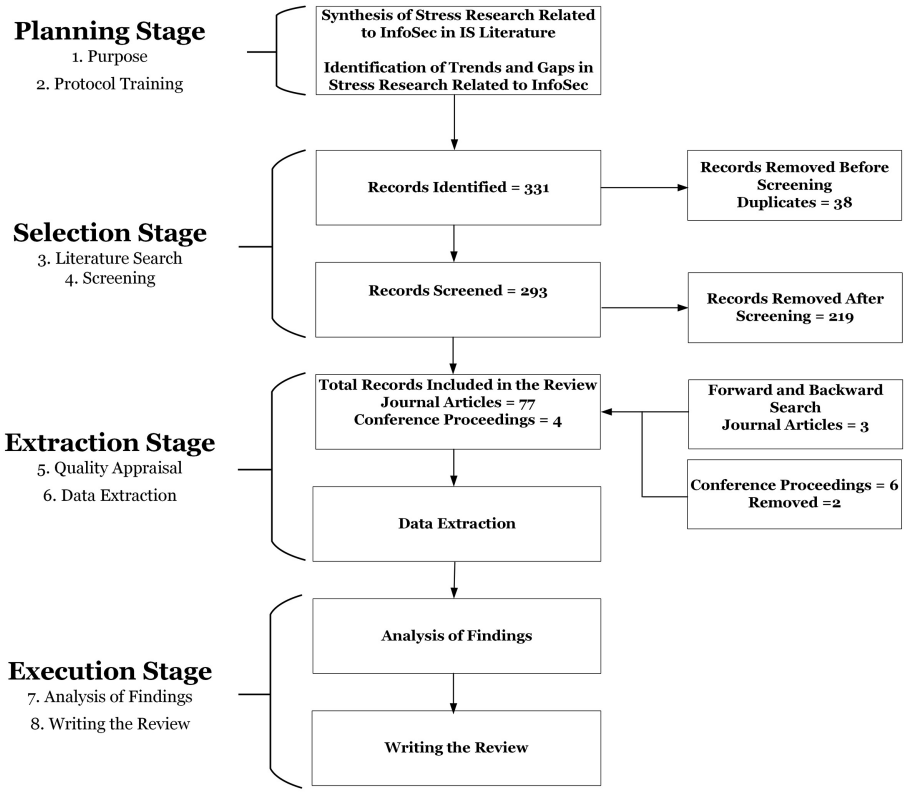
Additionally, cybersecurity professionals must often serve the role of the organizational "villain" (Zurkus, 2019) by imposing surveillance and monitoring technologies on their colleagues while maintaining the system and network controls that their fellow employees often view as impediments to productivity. When employees circumvent or violate these technologies or controls, it is the duty of the cybersecurity professional to alert authorities and, in many cases, enforce sanctions on the accused. This "guardian of the fence" role in organizations is unique to the cybersecurity profession and carries its own set of demands, stress responses and stress outcomes that deserve closer inspection.

As the study of stress among cybersecurity professionals has received little research attention, we sought to bring some initial clarity to this area. To this end, we first need to consider how stress has been approached by IS scholars in their study of IS and cybersecurity phenomena. To best reveal gaps and trends and illuminate potentially fruitful paths for future research, we conducted a review following the eight-step process suggested by Okoli and Schabram (2010) and Okoli (2015). We contend that extant general workplace and IS-specific stress literature can inform the study of stress experiences among cybersecurity professionals. Ultimately, this review culminates in actionable directions for future research on the study of stress among cybersecurity professionals. In the following sections, we describe the review process and findings, culminating in a set of associated future research opportunities.

2. Review process

We followed the literature review process of Okoli and Schabram (2010) and Okoli (2015). The steps of this review process are shown in Figure 1. We created a comprehensive stress literature corpus by including the articles from leading IS journals and conferences (Webster and Watson, 2002), and other domains of study where the relevant research may appear, such as computer science and management (Vom Brocke *et al.*, 2015). See Online Appendix 2, for the list of included journals.

Our review process covered approximately 30 years (1990–2020) of the research literature. The initial search was run in January 2020 and new articles were added during the review process. The initial corpus of the articles was created using relevant keywords based on the range of possible terms and a variety of database coverage (Tarafdar *et al.*, 2019). We referred to prior research on stress (such as work-related stress, technostress and security-related



Source(s): Okoli and Schabram (2010)

Figure 1.
Eight-step literature review process

stress (SRS)) to guide the selection of key terms (Fischer and Riedl, 2017; D'Arcy *et al.*, 2014; Tarafdar *et al.*, 2019; Li and Shani, 1991; Moore, 2000). Because every discipline has a unique lexicon for stress and to keep our search broad (at least initially), we used terms such as "stress" OR "strain" OR "work exhaustion" OR "burnout" OR "coping" OR "appraisal" OR "technostress" appearing within the abstract, keywords and title as our inclusion criteria. To overcome selection bias and add reproducibility and quality to our research, we follow prior stress research (Tarafdar *et al.*, 2019) by explicitly detailing the exclusion criteria we used and the resulting papers which were excluded in this process (see Appendix 2).

Consistent with the prior stress research, we used EBSCO as a search engine to search the databases of Academic Search Complete, Business Source Premier, and Business Source Ultimate (Tarafdar *et al.*, 2019). In addition, scholarly work was also obtained from Google Scholar. Using the initial set of broad terms allowed us to find articles that are not only related to technology – and hence technostress only – but also studies related to stressful experiences in technical careers, work-related stress, stress experiences from IT implementation, compliance with IT security technology, compliance with InfoSec policies, burnout and work exhaustion. The use of the initial set of broad search terms also allowed us to find articles related to stress in the InfoSec context as well. Also, the articles related to stress (physical, psychological and physiological), technostress, strain, work exhaustion and burnout experienced by working professionals from IT/IS and stress experienced because of job

environment characteristics are included. The articles that failed to mention the terms stress, strain, burnout or exhaustion, but are related to stress coping and appraisal (such as the appraisal of IT innovation and coping with the IT) in the workplace were also included.

Next, a forward search was performed to include articles that have been cited by articles identified in the initial search (Webster and Watson, 2002; Vom Brocke *et al.*, 2015). The journal of AIS Transactions on Replication Research was added through this forward search. Similarly, a backward search was performed to identify any articles cited by the selected articles (Webster and Watson, 2002). Because stress is a relatively new area of study for InfoSec scholars, we included articles published in the major IS conferences' proceedings. Our initial corpus of literature comprises 331 articles from 21 journals and six conferences (see Figure 1, and online Appendix 2 for further details). The findings of the execution of the review of these articles are presented next.

3. Review findings

This section summarizes the review findings related to the existing stress research in IS and InfoSec and uses that as a basis to develop future research on stress among cybersecurity professionals. We looked at McGrath's stress process (McGrath, 1970, 1976) as a guiding framework to summarize the articles and identify trends and gaps in the literature (see online Appendix 3 for a summary of included articles). McGrath's stress process (Figure 2) is well recognized in seminal texts (Cooper *et al.*, 2001; Folkman and Lazarus, 1985; Lazarus and Folkman, 1984, 1987; Kahn and Byosiere, 1992) and articulates a multistage process in which (1) an individual encounters an environmental demand [1], (2) which initiates an appraisal process in terms of its relevance to personal well-being, (3) which triggers stress responses in terms of psychological states (e.g. coping responses), and (4) which results in psychological, behavioral and physiological outcomes. This process describes the general stages of stress and allows for more nuanced views of each stage based on applicable theories.

Although the stages provided in McGrath's stress process are general, they manifest as context-specific phenomena in which demands are inherent to a particular context (Cooper *et al.*, 2001; Lazarus and Folkman, 1987). For example, within an organization, stressful work experiences can be associated with information security (D'Arcy *et al.*, 2014), technology development, technology adoption (Ayyagari *et al.*, 2011; Ragu-Nathan *et al.*, 2008; Windeler *et al.*, 2017; Beaudry and Pinsonneault, 2005) and work–life equilibrium (Moore, 2000; Ahuja *et al.*, 2007; Igbaria *et al.*, 1994; Li and Shani, 1991).

By leveraging McGrath's stress process as a framework for presenting our assessing review findings, we can explain how the stress research in IS and information security applies to the cybersecurity profession and explain how and why cybersecurity professionals respond to job demands in the manner they do. Further, McGrath's stress process allows us to reveal and highlight the critical areas of the process cybersecurity professionals undergo in dealing with stress that is either under-researched, in need of further exploration or plagued by a lack of consensus among scholars working in the area – all circumstances that can lead to a stagnation of knowledge among scholars attempting to contribute to our understanding of the phenomenon (Crossler *et al.*, 2018).

3.1 Demand

Adapting an existing definition, we define demands as events or characteristics of events that cybersecurity professionals encounter in the workplace (Kahn and Byosiere, 1992). Demands

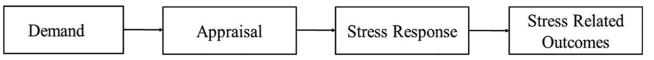


Figure 2.
McGrath's stress process

are neutral by nature, not necessarily seen as either good or bad. Further, demands can be physical or psychological (Simmons and Nelson, 2007). Within any organization, the demands that cause stress can be classified into different categories: physical demands (e.g. noise), job-related demands (e.g. work hours), role demands (e.g. role ambiguity, role conflict and role overload), relationship demands (e.g. relationships with supervisors, co-workers, etc.), career-related demands (e.g. job insecurity), work schedule–related demands (e.g. work shifts), organizational factors (e.g. organizational structure), traumatic events (e.g. a major accident), organizational change (e.g. a merger), work–family (or family–work) conflicts and invasions of privacy (Sonnentag and Frese, 2003; Ayyagari *et al.*, 2011; Cooper *et al.*, 2001). Additionally, technology-enabled interruptions, social media use at work, email (overload), IS project-related demands, computer monitoring and smartphone withdrawal have been explored by IS scholars as potential determinants of stress (Chen and Karahanna, 2018; Galluch *et al.*, 2015; Ragu-Nathan *et al.*, 2008; Tarafdar *et al.*, 2007; Tams *et al.*, 2018a; Windeler *et al.*, 2017; George, 1996).

Some demands are imposed by an organization's InfoSec requirements. We refer to them as security demands. Security demands can be in the form of policies, procedures and behavioral controls. Security demands can be technical, and nontechnical in nature. Security demands can also be internal when imposed by an organization's own InfoSec requirements or external due to government or industry mandates (D'Arcy *et al.*, 2014; Ament and Haag, 2016a; Lee *et al.*, 2016). Security demands can cause physical, cognitive and emotional overload among those who are tasked with attending to them (D'Arcy *et al.*, 2014, 2018).

3.1.1 Challenge and hindrance related demands. Our review finds a two-dimensional classification of demands in the form of the challenge and hindrance framework (CHF) (Cavanaugh *et al.*, 2000; LePine *et al.*, 2005). This framework describes demands as either challenge or hindrance related. In general, challenge demands are workplace demands or circumstances that are potentially stressful but produce positive work-related outcomes; however, hindrance demands are those that constrain or present an obstacle to an individual's work accomplishments and do not produce positive work-related outcomes (Podsakoff *et al.*, 2007; LePine *et al.*, 2004; Cavanaugh *et al.*, 2000). The CHF has recently been used in IS technostress research and classifies technology-related demands as challenge and hindrance technostressors (Califf *et al.*, 2020).

3.1.2 Technostress creators. The literature also reveals a set of demands referred to as technostress creators. Technostress creators are contextualized demands related to the use of information communication technology (ICT), capturing the overload (techno-overload), complexity (techno-complexity), invasiveness (techno-invasion), insecurity (techno-insecurity) and uncertainty (techno-uncertainty) dimensions of ICT use (Ragu-Nathan *et al.*, 2008; Tarafdar *et al.*, 2007). Demands are imposed by ICTs, where ICTs force users to work faster and for longer durations of time (techno-overload). ICTs appraised as complex require users to spend more time and effort learning new skills (techno-complexity). Further, ICTs perceived as invasive to users' privacy (techno-invasion) can cause a sense of fear among users that they could lose their jobs (techno-insecurity). Primarily, these ICT-imposed demands are associated with negative outcomes (Tarafdar *et al.*, 2007, 2010, 2015). For more than a decade, technostress creators have been explored in a variety of studies (Wang *et al.*, 2008; Fuglseth and Sørebø, 2014; Krishnan, 2017; Pirkkalainen *et al.*, 2019; Srivastava *et al.*, 2015). Overall, technostress creators are presented in the literature as a threat or hindrance to one's job or personal accomplishments (Tarafdar *et al.*, 2019).

3.1.3 Security-related stress (SRS) technostress creators. Technostress creators are further contextualized in the InfoSec as SRS and security-related technostress creators; however, only three dimensions of technostress creators – overload, complexity and uncertainty – have been deemed appropriate (D'Arcy *et al.*, 2014, 2018; Hwang and Cha, 2018; Hwang *et al.*, 2021). D'Arcy *et al.* (2014), the first article to contextualize technostress creators to the InfoSec

context, relabels these dimensions as SRS overload, SRS complexity and SRS uncertainty to make them more context-specific. Ament and Haag (2016a) extend D'Arcy *et al.* (2014) work and suggest that the demands imposed by an organization's security requirements cause stress through the invasion of privacy, conflicts as well as security-related news (such as data breaches). However, more recently, D'Arcy and Teh (2019) conceptualized SRS slightly differently from previous work and focused on the security requirements that vary daily and serve as hindrances or obstacles to an employee's primary task achievements.

3.2 Appraisal

An appraisal process refers to an individual's categorization and evaluation of demand regarding the appraiser's well-being (Lazarus and Folkman, 1984, 1987). A demand is positively appraised if it tends to support/enhance the appraiser's well-being and accomplishment of job tasks. A positive demand appraisal is also known as a challenge appraisal, with the outcome being deemed as a positive stressor or challenge stressor (Hargrove *et al.*, 2013, 2015; Califf *et al.*, 2020; LePine *et al.*, 2016). On the other hand, if a demand hinders the accomplishments of a job task and personal well-being, its appraisal is referred to as a negative appraisal or hindrance appraisal, and such demands are regarded as negative stressors or hindrance stressors (Hargrove *et al.*, 2013, 2015; Califf *et al.*, 2020). For example, consider the demand of evaluating new surveillance technology for deployment in an organization. If a cybersecurity professional is excited about the possibility of adding to his/her surveillance options, this task could be one that is challenging and perhaps even conducted under duress from a time and budget perspective but could serve as a challenge stressor because its overall effect is a positive one to the professional. For a different cybersecurity professional, with a different set of personality traits, the entire experience may produce an overall negative effect, which would qualify the demand as a negative stressor. The appraisal process is core to the theories that aim to explain what happens during a stress process. These theories use slightly different terms to describe the appraisal process. Still, the essence of each is that once encountered with a demand; an individual performs a cognitive assessment of it. From three different theoretical viewpoints, we discuss examples of the appraisal process.

3.2.1 Demand appraisal as per transactional theory of stress. The transactional theory of stress suggests that individuals engage in primary and secondary appraisal processes (Lazarus and Folkman, 1987). During the primary appraisal of a demand, an individual considers the demand in terms of its relevance to his/her well-being and whether it presents a challenge or opportunity to improve his/her well-being or if it is seen as a hindrance or threat that is detrimental to his/her well-being. During the secondary appraisal, an individual assesses the level of control he/she has over the demand and available coping (adaptation) choices relative to the resources available to deal with the demand (Lazarus and Folkman, 1987; Beaudry and Pinsonneault, 2005; Galluch *et al.*, 2015). Alternatively, if the individual considers the demand to be irrelevant in the primary appraisal, the secondary appraisal is not needed.

For an InfoSec event, a perceived threat represents a primary appraisal; during the secondary appraisal, a determination is made regarding how to avoid the threat (Liang *et al.*, 2019). SRS is positioned as a negative stressor resulting from the primary and secondary appraisal process (D'Arcy *et al.*, 2014, 2018; Ament and Haag, 2016a, b). Overall, SRS is considered a hindrance stressor, arising when employees appraise InfoSec requirements as an obstacle to their primary job tasks and react to them with frustration and fatigue (D'Arcy and Teh, 2019).

3.2.2 Demand appraisal as per cybernetic theory. Similarly, cybernetic theory explains that demands are appraised in terms of their ability to serve as discrepancy-reducing or

discrepancy-enhancing mechanisms (Stich *et al.*, 2019a; Edwards, 1992). For example, a cybersecurity professional receiving more security alerts than he/she desires to deal with may attempt to shut down the alert system or ignore the alerts. In this situation, this professional is trying to distance himself/herself from the source of stress, known as a discrepancy-enhancing mechanism and the imposed demand is deemed as a hindrance stressor. However, in a similar situation, if the cybersecurity professional attempts to troubleshoot the cause of the alerts, then he/she is attempting to reduce the discrepancy between the desired and current state of the demand, which is known as a discrepancy-reducing mechanism (Liang and Xue, 2009). Here, the imposed demand is deemed to be a challenge stressor.

3.2.3 Demand appraisal as per person-environment fit (P-E fit) theory. P-E fit theory offers an alternative perspective on demand appraisals (Edwards and Cooper, 1990). P-E fit theory contends that people try to achieve and maintain equilibrium in terms of their preferences and needs being balanced or in alignment with their environment's ability to satisfy those needs or in terms of the demands of the environment and their ability to satisfy or meet those demands. When this equilibrium is disturbed or becomes imbalanced, people become stressed. This state of disturbance or imbalance between a person and his/her environment is referred to as a misfit (Edwards, 1996; Edwards and Cooper, 1990) and is thought to be based on the subjective evaluation of whether one's needs are not being met or that one is incapable of meeting the expectations and demands of the environment (Ayyagari *et al.*, 2011; Chilton *et al.*, 2005; LeRouge *et al.*, 2006; Stich *et al.*, 2019b; Wang *et al.*, 2020; Lee *et al.*, 2016).

3.3 Stress response

Stress responses are the physical and psychological responses to challenge and/or hindrance stressors that result from demand appraisals; they are relative to an individual's mental and emotional state (Cooper *et al.*, 2001). Although, for any given demand, both positive and negative stress responses can occur (Califf *et al.*, 2020), our review findings reveal that the primary focus of stress research has been on negative stress responses (Tarafdar *et al.*, 2019). Next, we discuss the stress responses as they emerged in our review process.

3.3.1 Coping. One of the dominant labels associated with stress responses in the literature is coping. Coping is broadly defined as a "cognitive and behavioral process of mastering, tolerating, and reducing internal and external demands" (Cooper *et al.*, 2001). By applying the term coping response, scholars are trying to convey a physical and psychological response to a demand appraisal (D'Arcy *et al.*, 2014, 2018; D'Arcy and Teh, 2019; Galluch *et al.*, 2015; Liang *et al.*, 2019; Beaudry and Pinsonneault, 2005; Lazarus and Folkman, 1984, 1987).

3.3.1.1 Problem-focused and emotion-focused coping. Our review of the stress literature in IS and InfoSec reveals a framework for coping responses in which responses have been classified as either problem or emotion-focused (Lazarus and Folkman, 1984; Beaudry and Pinsonneault, 2005; Liang *et al.*, 2019). Using this framework, when a demand is perceived as an opportunity (challenge), a problem-focused coping response is induced, in which the demand is elaborated on, and positive responses, such as exhilaration or focus, are formed in an effort to extend or savor the demand. For example, when new surveillance technology is introduced, it may be seen as a challenge or opportunity by cybersecurity professionals. In this circumstance, a coping response to it would likely be one such as anxiousness, elation or increased concentration – which are responses associated with maximizing the benefits they accrue from the new technology. Other problem-focused coping responses in the context of IT security threats are adopting safeguard measures such as password updates, removal of cookies, encryption, use of antivirus software and so forth (Liang and Xue, 2009).

Alternatively, when a demand is perceived as a threat (or hindrance), an emotion-focused coping response is evoked in the form of anxiety, fear or nervousness, which is reflective of the negative stress the demand has produced (Liang *et al.*, 2019; Beaudry and Pinsonneault, 2005; Lazarus and Folkman, 1984). For example, if appraised as a hindrance, the same surveillance technology will induce a form of negative stress, such as worry, fatigue, burnout or moral disengagement. Moral disengagement and neutralization from InfoSec policies are other forms of emotion-focused coping responses, which are a form of distress caused by negatively appraised hindrance security demands (D'Arcy *et al.*, 2014; D'Arcy and Teh, 2019).

3.3.1.2 Coping adaptiveness. Our review findings also highlight an important, albeit rarely tested, a caveat in how coping responses are intertwined. Research shows that in the event of InfoSec threats (as security demands), people engage in both problem-focused and emotion-focused coping responses; however, as people engage in emotion-focused coping responses, it affects their problem-focused responses (Liang *et al.*, 2019). For example, when people experience the risk of being victimized by phishing attacks, multiple coping responses may be triggered: a problem-focused coping response, such as curiosity, and emotion-focused coping responses, such as worry. These coping responses have been shown to form a higher-order construct called coping adaptiveness, which manifests in the form of increased task-focused coping and a decrease in emotion-focused coping and avoidance coping (Wang *et al.*, 2017).

3.3.1.3 Proactive and reactive coping. Our review also revealed another form of stress response known as proactive coping. When a demand is appraised as a hindrance stressor and cannot be avoided, people know they are going to face it sooner or later and proactively prepare themselves for it. The alternative to proactive coping is an emotional, reactive coping response (Pirkkalainen *et al.*, 2019). When proactively coping, people mentally prepare themselves for the stressful demand or develop resilience toward the demand so that their coping responses can be more positive, whereas when reactively coping, people are more likely to be distressed if the demand is negatively appraised (Pirkkalainen *et al.*, 2019).

3.3.2 Burnout. Burnout is a state of exhaustion and cynicism typically associated with person-related demands, which has also been shown to entail decreased personal efficacy (Maslach and Jackson, 1981). Burnout has three dimensions as exhaustion, cynicism and personal efficacy (Maslach and Jackson, 1986). InfoSec context defines security compliance burnout as a contextualized form of burnout that employees experience as they attempt to comply with their organization's InfoSec demands (Pham, 2019).

3.3.3 Information security stress. Information security stress (ISS) is a stress response that results from a misfit between the security goals that exceed employees' capabilities as they attempt to comply with their organization's security requirements (Lee *et al.*, 2016). An organization's enhanced security requirements can cause work overload and a sense of privacy invasion, resulting in ISS.

3.3.4 Interruption overload. Interruption overload results from work-related interruptions. When employees receive more work-related interruptions than they can handle, they appraise those interruptions as stressful (Chen and Karahanna, 2018).

3.3.5 Role stress. Finally, our review findings reveal a form of stress response related to role stress. Role stress emerges from the appraisal of demands associated with role ambiguity, role conflict and role overload (Hwang and Cha, 2018; Tarafdar *et al.*, 2007; Igbaria *et al.*, 1994; Igbaria and Guimaraes, 1993; LeRouge *et al.*, 2006). The positive role stress responses that have been studied in the literature include job engagement, job satisfaction, career satisfaction, career advancement prospects (such as the likelihood of promotability), developmental prospects such as expectations regarding the job opportunities for challenging assignments and potential for recognition (Srivastava *et al.*, 2015; Califf *et al.*, 2020; Igbaria and Guimaraes, 1993; Armstrong *et al.*, 2015; Igbaria *et al.*, 1994; LeRouge *et al.*, 2006; Shropshire and Kadlec, 2012).

3.3.6 Savoring. Stress responses can be positive in response to demands appraised as opportunities or challenges; this form of stress response is also referred to as savoring (Simmons and Nelson, 2007). Savoring is defined as one's capacity to "attend to, appreciate and enhance positive experiences" in one's life (Bryant and Veroff, 2007).

3.4 Stress-related outcomes

A key differentiator of stress responses and stress-related outcomes is that stress responses are reactions, rather than actions. Stress related outcomes (actions) are formed after a stress response to affect demand and subsequent demand appraisals. Stress-related outcomes are behavioral and physiological, such as changes in heart rate, lack of sleep, depression, fatigue, etc. However, behavioral outcomes are primarily studied; hence this review focuses on those responses. Behavioral outcomes include job performance, productivity and even job turnover (Tarafdar *et al.*, 2007; Zhao *et al.*, 2020). Many different stress-related outcomes can be seen; a few of them are addressed here.

Our review of the stress literature reveals that (negatively) stressed employees have a low willingness to use technology or are less willing to adopt new technology for improving performance or unwilling to extend the use of available technological solutions (Fadel, 2012; Beaudry and Pinsonneault, 2010; Fuglseth and Sørebø, 2014; Califf *et al.*, 2020). Similarly, in InfoSec, stressed employees have a lower intent to comply with InfoSec policies (Ament and Haag, 2016a; D'Arcy *et al.*, 2014, 2018; D'Arcy and Teh, 2019; Pham *et al.*, 2016; Trang and Nastjuk, 2021). In this sense, compliance or noncompliance is a type of stress-related outcome.

Job turnover as stress-related outcome is well-suited to the study of stress among cybersecurity professionals (Igbaria and Guimaraes, 1993; Moore, 2000; Joseph *et al.*, 2007; Ahuja *et al.*, 2007; Armstrong *et al.*, 2015). Job turnover is defined as voluntarily leaving a job for a similar job with another employer and is one of the most common stress-related outcomes receiving attention from IS scholars, though not yet in the unique context of the cybersecurity profession (Joseph *et al.*, 2007). Research shows that general IS professionals experiencing a high level of stress in the form of burnout and work exhaustion have a higher intent to leave their jobs or – in the extreme case – the IS profession overall (Shih *et al.*, 2011; Podsakoff *et al.*, 2007; Moore, 2000; Ahuja *et al.*, 2007; Califf *et al.*, 2020; Rutner *et al.*, 2008).

Strain is a long-term stress response among professionals experiencing high stress. A prolonged state of strain, work exhaustion or burnout influence employees' effectiveness, efficiency, decision quality and decision accuracy (e.g. phishing email detection accuracy) (Monica and Gloria, 2019; Wang *et al.*, 2017) while impacting their overall productivity, personal accomplishments, team performance and job performance (Pirkkalainen *et al.*, 2019; Zhao *et al.*, 2020; Tarafdar *et al.*, 2007, 2010; Helkala *et al.*, 2016; Windeler *et al.*, 2017; Venkatesh *et al.*, 2018; Tams *et al.*, 2014, 2018b; Shih *et al.*, 2013; Moody and Galletta, 2015; Yu *et al.*, 2018); all stress response outcomes apply to the study of stress among cybersecurity professionals. In extreme cases, long-term negative health consequences have also been reported (Budnick *et al.*, 2020; George, 1996; Fadel, 2012; Beaudry and Pinsonneault, 2010; Fuglseth and Sørebø, 2014; Moore, 2000).

4. Future research opportunities

Based on our synthesis and interpretation of the previously reviewed literature, the following section presents our suggested opportunities for future research on stress in the cybersecurity profession, detailing what we need to learn more about in terms of the demands, appraisal, stress responses and stress-related outcomes related to cybersecurity professionals. Figure 3 depicts the opportunities for future research relative to McGrath's (1970) stress process, which served as a guiding framework for presenting this review's

findings. Figure 3 is complemented by Table 1, which summarizes the opportunities and the underlying observations from the literature that motivates them.

4.1 Opportunity 1: Cybersecurity scholars should investigate the unique security demands faced by cybersecurity professionals

The demands faced by cybersecurity professionals appear distinct from those experienced by ordinary working professionals or IT/IS professionals not responsible for an organization's security. Yet, our broad observation of the stress research reveals those demands have not yet been identified or at least contextualized to the cybersecurity profession.

The security demands required of cybersecurity professionals can be both technical and nontechnical. Technical security demands involve the installation and maintenance of security appliances such as firewalls, antimalware software, security orchestration, automation and response (SOAR) solutions, security information and event management (SIEM) solutions, and others. Nontechnical security demands involve the creation and enforcement of policies, standards or other activities designed to support and govern an organization's security posture.

For technical security demands, scholars should consider the characteristics of technology highlighted in the technostress and InfoSec literature, including technical complexity, reliability, interoperability and false-positive rates (Ayyagari *et al.*, 2011; Cavusoglu *et al.*, 2005). However, there are other characteristics that have not yet been explored that are salient to the cybersecurity professional context, including noise, chattiness and versatility. Noise and chattiness refer to the reporting nature of devices, where some devices often communicate with a server, creating much network overhead; some of it is quite useless, thus becoming noise. The versatility of a network appliance refers to its ability to serve multiple functions within an overall technology infrastructure – such as a network router that can shape network traffic as well as detect and respond to suspicious ingress and egress traffic.

Security controls in the form of employee monitoring and surveillance are often seen as invasive and threatening to the privacy of employees (Posey *et al.*, 2011; Ament and Haag, 2016a, b), creating a burden on cybersecurity professionals to help manage any subsequent resulting employee discord. For this reason, surveillance technologies may have an adversarial characteristic unique to the cybersecurity profession that captures the negative impact they can have on their relationships with their fellow colleagues.

Similarly, scholars should consider the nontechnical security demand characteristics not yet explored in the stress literature. These characteristics may include complexity, invasiveness or vagueness, among others. For instance, InfoSec policies and procedures are often complex because the technical jargon presented in InfoSec policies is difficult to understand and requires cybersecurity professionals to spend time and effort to learn and relearn them. Further, just like technical demands, nontechnical security demands, such as InfoSec policies and procedures, may also compromise the privacy of employees (D'Arcy *et al.*, 2014; D'Arcy and Teh, 2019; Ament and Haag, 2016a, b), hence generating hostility in the employee workforce that can weigh on the psyche of a cybersecurity professional (Posey *et al.*, 2014).

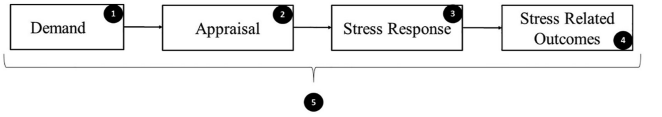


Figure 3.
Future research opportunities mapped to McGrath's (1970) stress process

Opp #	Opportunity/Potential research questions	Motivating observation
1	Investigate the unique security demands faced by cybersecurity professionals Potential research question: *RQ1: What are the unique security demands faced by cybersecurity professionals?*	Cybersecurity professionals experience both technical and nontechnical security demands. For technical security demands, the unexplored characteristics of security technology involve interoperability, noise, rate of false alarms, chattiness and versatility. Adversarial characteristics of security controls and management of employee discord are another form of demand that cybersecurity professionals uniquely experience Similarly, the nontechnical demands imposed by ever-changing InfoSec security policies and procedures present another unique category of demands experienced by cybersecurity professionals, requiring a continuous investment of time and effort to learn and relearn how to comply with them
2	Explore the appraisal process that cybersecurity professionals follow in assessing security demands Potential research questions: *RQ1: How do organizational and individual characteristics interact with the characteristics of technical and nontechnical security demands in the demand appraisal process?* *RQ2: What individual and organizational characteristics increase the likelihood that cybersecurity professionals will appraise a given security demand (technical or nontechnical) as a challenge stressor?* *RQ3: What individual and organizational characteristics increase the likelihood that a given security demand (technical or nontechnical) will be appraised as a hindrance stressor by cybersecurity professionals?*	Regardless of the theoretical underpinning, a broad notion of the cognitive stress paradigm is that individuals cognitively appraise environmental demands (Lazarus and Folkman, 1984). However, the stress literature applicable to the study of stress among cybersecurity professionals revealed that demand appraisals have been given limited attention among scholars (see Appendix 3). When attended to, demand appraisals have been explained primarily through one of three theoretical lenses (transactional theory of stress, P-E fit theory and cybernetic theory), in which individuals perform a subjective evaluation of their environment in terms of opportunity or threat (D'Arcy *et al.*, 2014, 2018; Galluch *et al.*, 2015; Liang *et al.*, 2019), (mis)fit (Ayyagari *et al.*, 2011; Stich *et al.*, 2019b; Chilton *et al.*, 2005), or (in) equilibrium (Stich *et al.*, 2019a) However, what has lacked the most attention is the explanation of the factors that may influence the demand appraisal process for cybersecurity professionals and how certain factors are more influential than others, creating a challenge or hindrance perception of demand. Some early research suggests that age, gender and personality differences can play an influential role in the stress process, but we have an underdeveloped understanding of how these differences affect cybersecurity professionals' appraisal of demands (Ragu-Nathan *et al.*, 2008; Tams *et al.*, 2017; Srivastava *et al.*, 2015; Maier *et al.*, 2019; Hwang and Cha, 2018; Lazarus and Folkman, 1987). Most research that has considered individual differences has shown how these differences affect the overall experience of stress but not the influence on the appraisal process itself, but cybersecurity professionals are a unique breed of IT professional (Cobb, 2016; Bashir *et al.*, 2017) and therefore deserving of special consideration
3	Explore the multitude of stress responses cybersecurity professionals engage in following a demand appraisal Potential research question: *RQ1: How do cybersecurity professionals savor and cope with the IT security demands of their organizations?*	Most studies on stress in a security-related context have applied technostress concepts to SRS research. Commonly studied stress responses in technostress research are negative (see Appendix 3) primarily because technostress has been positioned as a dark side of stress phenomenon (Tarafdar *et al.*, 2019). This limitation has also extended to SRS research. Frustration, fatigue and moral disengagement are some negative stress responses studied in the SRS context. But this limitation presents an opportunity for future research to focus on positive stress responses among cybersecurity professionals, which can manifest as excitement, hope, trust, job engagement, etc. (Simmons and Nelson, 2001, 2007)

(*continued*)

Table 1.
Future research opportunities summary table

Opp #	Opportunity/Potential research questions	Motivating observation
4	Study novel stress outcomes Potential research question: *RQ1: What are the most salient stress related outcomes associated with the cybersecurity profession?*	A key observation from our review is that the conceptualization of stress in the InfoSec domain adds a new perspective to behavioral security research, which focuses primarily on the determinants of information security policy (ISP) violations and noncompliant behaviors. Being rooted in an ISP compliance perspective, InfoSec stress research primarily focuses on policy compliance issues as an outcome variable (for example, (D'Arcy and Teh, 2019; Nasirpouri Shadbad and Biros, 2021; Hwang and Cha, 2018; Pham *et al.*, 2016) leaving an unexplored area of investigation in studying the influence of SRS on other organizational variables such as job satisfaction, productivity, turnover and so forth. Beyond compliance issues, other outcome variables that have emerged in our review are security compliance burnout and information security awareness (McCormac *et al.*, 2018; Pham *et al.*, 2016; Pham, 2019) However, for all of these compliance and compliance-related variables, their influence on the generation of stress among cybersecurity professionals has gone unexplored. Cybersecurity professionals are on the enforcement side of ISPs, and the stress they encounter should result in a unique set of stress related outcomes. Future research is needed to determine what those outcomes are and how stress plays a role in influencing them
5	Practice theoretical pluralism in studying stress among cybersecurity professionals	Even though research on stress among cybersecurity professionals and in the broader context of InfoSec is still developing, we have found richness in the theoretical perspectives used. This is a somewhat surprising observation, given that a lack of theoretical richness has been suggested as a limitation of the technostress literature (Tarafdar *et al.*, 2019). Yet to its credit, the research that would be applicable to inform a study of stress among cybersecurity professionals exhibits no such limitations and should provide a robust theoretical spectrum from which to conduct future research. We find theories such as moral disengagement theory (MDT) and coping theory, person–organization (P-O) fit theory and transactional theory of stress has been used to explore SRS- and ISS-related phenomena, respectively (Lee *et al.*, 2016; D'Arcy *et al.*, 2014). Affective event theory and coping theory have been applied to understand how security demands can be conceptualized as hindrance stressors (D'Arcy and Teh, 2019). The job demands-resource model has been used to explain information security compliance burnout (Pham *et al.*, 2016; Pham, 2019)

Table 1.

Cybersecurity professionals typically encounter demands in some very specific, contextualized manner. For example, the most common reason employees use social media at work is to take a mental break and network (Olmstead *et al.*, 2016). However, for cybersecurity professionals, social media is not a tool to relieve distress, but it is a source of threat intelligence to gather information regarding vulnerabilities, malware and potential threats that may pose a significant risk to their organization (Kropotov and Yarochkin, 2019). In the meantime, cybersecurity professionals also need to monitor the social media use of general employees and enforce the policies and sanctions that guide the restrictions. Additionally, cybersecurity professionals have the unique experience of encountering demands that most would classify as hindrance demands, but for them, they could be challenge-oriented. For example, consider workplace surveillance cameras. These cameras are most likely regarded as a hindrance for a regular employee. Still, for a cybersecurity professional, they are most likely a challenge demand because they can help identify potentially malicious activities in action.

For these reasons, we suggest scholars ask:

RQ1. What are the unique security demands faced by cybersecurity professionals?

4.2 Opportunity 2: Cybersecurity scholars should further explore the appraisal process that cybersecurity professionals follow in assessing security demands

Based on the extant stress literature, a demand appraisal process should prepare cybersecurity professionals to take actions in the form of stress responses (Lazarus and Folkman, 1987). Hence, to understand the impetus for stress responses among that population, it is imperative first to understand how cybersecurity professionals appraise security demands. Specifically, it is crucial to identify the key characteristics of the demands themselves (as outlined in the opportunity 1), which weigh in on the appraisal process, as well as the key characteristics of the organizational environment in which the demands occur and of the cybersecurity professional involved in appraising these demands. The key organizational characteristics that can influence appraisal process can include organizational complexity, uncertainty, cohesiveness and mindfulness, job autonomy among others (Johnston *et al.*, 2019; Jensen *et al.*, 2017). Understanding how demand and organizational characteristics interact during appraisal process and the methods best suited for testing their interaction is equally crucial.

Organizational factors such as organizational climate, workgroup characteristics and job characteristics also serve as situational variables that can influence how a demand is appraised (Cooper *et al.*, 2001). Another organizational characteristic of interest, job autonomy – or job-decision latitude – refers to the control people have over their jobs in terms of their freedom, independence and discretion for how to respond to job demands (Karasek, 1979). When job autonomy is high, general IT professionals experience low levels of work exhaustion (Moore, 2000; Ahuja *et al.*, 2007; Armstrong *et al.*, 2015). A high level of job autonomy in IT-related careers motivates IT professionals to learn new behaviors and lessen work exhaustion and job turnover intentions (Shih *et al.*, 2011). Therefore, given the appropriate level of job autonomy, cybersecurity professionals will be more likely to appraise a demand as a challenge stressor (Galluch *et al.*, 2015; Tams *et al.*, 2018a, 2020), but this influence, much like those provided by the other organizational characteristics presented above, is untested among cybersecurity professionals and is deserving of scholarly attention.

Finally, the cybersecurity professionals' individual characteristics cannot be ignored in the security demands appraisal process (Srivastava *et al.*, 2015; Krishnan, 2017). Individual characteristics such as personality traits or dispositions determine how people perceive their environment and react to it (Lazarus and Folkman, 1987). Cybersecurity professionals are a unique breed of professional (Bashir *et al.*, 2015) often having personality characteristics similar to the cyber violators they seek to identify and catch (Bashir *et al.*, 2017; Pfleeger and Pfleeger, 2012). In general, some people tend to become more stressed than others, leading to different appraisal outcomes (Maier *et al.*, 2017, 2019). Personality is generally conceptualized as being hierarchical (Maier *et al.*, 2019), with many specific and even context-specific traits (e.g. IT mindfulness; Maier *et al.*, 2019) being organized under a limited set of broad traits known as the Big Five. Broad traits are context-free, relatively stable and explain behavior or belief less precisely. In contrast, context-specific traits are often dynamic, narrower traits, helping us understand beliefs and behaviors in certain contexts, such as cybersecurity. Dynamic traits can also be influenced by experience. Research shows that people high in neuroticism, a broad trait, tend to appraise work demands more along the lines of hindrance stressors and are more prone to experience job burnout (Maier *et al.*, 2019; Srivastava *et al.*, 2015).

On the other hand, people high in stable and dynamic traits appraise work demands as challenge stressors and experience lower stress levels (Maier *et al.*, 2019). Being malleable and

having the strongest impact on work demands, dynamic context-specific traits can be developed or mitigated depending on organizational conditions or interventions. Given the dynamic nature of security threats, mindfulness among cybersecurity professionals can bring them out of "autopilot mode" in their appraisal of security demands, helping them to see security threats as something other than hindrance stressors. However, these characteristics of cybersecurity professionals have gone mostly unexplored in their role in the demand appraisal process and, as such, are deserving of the attention of scholars.

4.2.1 Opportunity 2.1: Cybersecurity scholars should leverage a variety of research designs and methods to explore demand appraisal process. Stress is a context-specific phenomenon where situational specifics influence the demand appraisal process and the associated stress-related outcomes (Lazarus and Folkman, 1984), thus warranting diverse research designs and research methods to address the research questions. In this regard, scholars can include both subjective (self-reported measures through surveys) and objective measures (physiological and neurobiological methods) of demand characteristics while exploring the demand appraisal process and the stress phenomenon as a whole. D'Arcy *et al.* (2014) note a critical limitation in InfoSec research focusing on only self-reported measures, calling for future research to practice more methodological pluralism in investigating the stress phenomenon. We argue that this methodological pluralism is critical to understanding cybersecurity professionals' demand appraisal process. Practicing methodological pluralism, Tams *et al.* (2014) compare the stress responses from self-reported and physiological measures (salivary α-amylase) and find that physiological measures of stress explain variance in the performance of a computer-based task beyond what could be explained by self-reported measures alone. Tams *et al.* (2014) conclude that self-reported and physiological measures do not correlate and can explain the conscious and unconscious aspects of stress, respectively. Other physiological indicators useful in stress research are galvanic skin response, blood cortisol level (commonly known as the stress hormone), heat flux, near-body temperature and skin temperature (electrodermal conductivity) (Moody and Galletta, 2015). During a stressful encounter, blood cortisol levels rise, and the skin becomes a better conductor of electricity because of the increased activity of sweat glands (Moody and Galletta, 2015). However, it is unknown whether similar physiological measures are activated in a demand appraisal process, which is a gap in current knowledge that is worthy of the attention of scholars.

Another potential path for future research may involve more attention to NeuroIS research which can help identify which regions of the brain and hormones are activated during a demand appraisal (Anderson *et al.*, 2016). NeuroIS research applies cognitive neuroscience and associated physiological measures to the study of IS phenomena (Dimoka *et al.*, 2011). The application of NeuroIS to the study of information security phenomena is known as neurosecurity (Anderson *et al.*, 2016). NeuroIS has been recognized for its ability to help scholars understand security behaviors, including stress-related phenomena (Riedl *et al.*, 2014; Anderson *et al.*, 2016). For example, Warkentin *et al.* (2016) have determined that fear appeals activate several areas of the brain associated with self-referential thinking. In another study, Vance *et al.* (2014) use electroencephalography (EEG) to understand how users perceive and respond to information security threats. Like other NeuroIS methods, eye-tracking techniques capture unconscious deep emotions. Through this technique, Vance *et al.* (2014) show that habituation occurs because of repeated exposure to security warnings, while Anderson *et al.* (2016) show that people unconsciously scrutinize repeated security warnings. The evidence from these studies suggests that if applied to the study of cybersecurity professionals' demand appraisal process, NeuroIS techniques would likely yield fruitful results.

In summary, scholars have a clear opportunity to engage in research exploring the process cybersecurity professionals follow in assessing security demands. Based on the opportunity

outlined above, we present the following research questions as suggestions for advancing scholarship in this area:

RQ1. How do organizational and individual characteristics interact with the characteristics of technical and nontechnical security demands in cybersecurity professionals' demand appraisal process?

RQ2. What individual and organizational characteristics increase the likelihood that cybersecurity professionals will appraise a given security demand (technical or nontechnical) as a challenge stressor?

RQ3. What individual and organizational characteristics increase the likelihood that a given security demand (technical or nontechnical) will be appraised as a hindrance stressor by cybersecurity professionals?

4.3 Opportunity 3: Cybersecurity scholars should explore the multitude of stress responses cybersecurity professionals engage in following a demand appraisal

In the organizational behavior literature, the holistic stress model by Simmons and Nelson (2007) explains the positive and negative psychological responses in the form of emotions, attitude and behavior. Positive emotional states are represented by feelings of joy, happiness and excitement, whereas a negative stress response takes the form of anger, anxiety and frustration. A feeling of hope, meaningfulness and vigor are a few examples of a positive attitude, whereas a negative attitude manifests in burnout and work exhaustion. The behavioral responses associated with positive states include work engagement and positive organizational citizenship behavior, while revenge, incivility and noncompliance behavior are the behavioral responses associated with negative psychological states (Aggarwal and Dhurkari, 2023). Depending on the psychological states derived from a demand appraisal, a cybersecurity professional will experience both the positive and negative psychological responses directed at mitigating/alleviating the negative psychological state, that is, coping or intensifying or enjoying a positive psychological state or savoring the positives (Simmons and Nelson, 2007; Lazarus and Folkman, 1987).

The essence of this discussion is that an individual's coping/savoring responses vary depending on his/her assessment of the demand, but overall, in the event of the security demand, a cybersecurity professional either approaches it in a problem-focused or emotion-focused manner or takes a hybrid approach of the two to increase his/her effectiveness and efficiency while minimizing the negative consequences of an InfoSec event and restoring emotional stability (Liang *et al.*, 2019; Beaudry and Pinsonneault, 2005). Overall, future research opportunities exist for identifying the coping and savoring responses in a cybersecurity profession context, how these relate to nondisruptive and disruptive security technology, and whether these responses vary by discrepant IT events in the security context. Hence, future research can attempt to answer these questions along with the following broad question:

RQ1. How do cybersecurity professionals savor and cope with the IT security demands of their organizations?

4.4 Opportunity 4: Cybersecurity scholars should seek to study novel stress outcomes

Another key observation from our review is that the conceptualization of stress in the InfoSec domain adds a new perspective to behavioral security research, which focuses primarily on the determinants of information security policy (ISP) violations and noncompliant behaviors. Being rooted in an ISP compliance perspective, InfoSec stress research primarily focuses on policy compliance issues as an outcome variable (for example (D'Arcy and Teh, 2019;

Nasirpouri Shadbad and Biros, 2021; Hwang and Cha, 2018; Pham *et al.*, 2016; Aggarwal and Dhurkari, 2023), leaving an unexplored area of investigation in studying the influence of stress on other organizational variables such as job satisfaction, employee productivity and turnover.

Beyond compliance issues, other outcome variables that have emerged in our review are security compliance burnout, and information security awareness (ISA) (McCormac *et al.*, 2018; Pham *et al.*, 2016; Pham, 2019). Security compliance burnout is experienced when employees comply with their organization's InfoSec policies and when there is a lack of organizational and personal resources to cope with security demands (Pham *et al.*, 2016; Pham, 2019). ISA is an understanding of an organization's InfoSec policies, rules and guidance. With a high level of ISA, employees can better perform secure computing behavior (McCormac *et al.*, 2018). Finally, we have found that ISA is also conceptualized as an outcome variable caused by the invasion of privacy and work overload from an organization's security requirements. However, beyond ISA, job satisfaction, employee productivity and turnover, there are other outcomes, such as burnout, regret and disgruntlement that are associated with the cybersecurity profession and have not been explored in that context. Moreover, as cybersecurity professionals are often charged with ensuring employees are abiding by ISPs, understanding these individuals' satisfaction, etc., as it pertains to the organizational ISPs would be a worthy endeavor, given that such factors may contribute to stress among this population. Hence, future research could benefit from the exploration of the following research question:

RQ1. What are the most salient stress-related outcomes associated with the cybersecurity profession?

4.5 Opportunity 5: Cybersecurity scholars should continue to practice theoretical pluralism in studying stress among cybersecurity professionals

We note that multiple theoretical perspectives have been used to understand SRS, ISS and information security burnout, among other stress-related phenomena. However, we have also noticed several understudied areas of the stress process, such as the characteristics of security demands that are deemed stressful for cybersecurity professionals, the demand appraisal process, stress responses and stress-related outcomes.

Theoretical pluralism allows studying the various micro and macro aspects of stress phenomena from different perspectives. For example, the transactional theory of stress guides understanding cognitive and behavioral efforts performed by cybersecurity professionals to cope with and savor the security demands in their work environment. The job demands-resources (JD-R) theory provides guidance for understanding the effects of security demands on cybersecurity professionals, where the unique effects of security demands and resources exhibit themselves in the form of work engagement, organizational commitment, job performance, motivation and burnout, among other forms (Pham *et al.*, 2016; Pham, 2019).

The cybernetic theory of stress and coping focuses on discrepancy-reducing and discrepancy-enhancing mechanisms; that is, a cybersecurity professional engages in the mechanism that reduces or increases the distance between the current and desired states here depending on the stressor (Edwards, 1992). Cybernetic theory can form an excellent theoretical lens to explore the adoption of new security technology within an organization because the goal is to decrease the discrepancy between the desired and current mental state of the cyber professional when it comes to the new technology.

P-E fit theory characterizes stress as a lack of correspondence between the characteristics of a person (e.g. abilities and values) and the environment (e.g. demands and supplies). This lack of fit can result in the unmet needs of cybersecurity professionals or job demands, which

ultimately results in deleterious psychological, physiological and behavioral outcomes. P-E fit theory is a multidimensional theory that suggests people (personality, values, skills, goals, emotions, etc.) and the environment, including the organization where cybersecurity professionals are employed, is multidimensional (e.g. organizational culture, expected behavior, pay structure, etc.) (Edwards and Billsberry, 2010). Similarly, cybersecurity professionals are nested within different levels of organizational dimensions. For example, cybersecurity professionals work in groups on different projects (person–people fit) and with different security technologies (person–technology fit) at the same time. However, using one kind of fit approach illuminates only one side of the stress phenomenon. P-E fit theory is an excellent way to demonstrate how different organizational factors create different security demands (e.g. outdated technology, lack of management support for security functions, etc.) and how the different dimensions of P-E (mist)fit lead to varying levels of psychological responses among cybersecurity professionals.

5. Discussion

Cybersecurity professionals represent a unique subset of IT professionals whose job roles focus on the defense of physical and digital assets from a persistent and ever-changing set of threats. However, how cybersecurity professionals assess these stressful experiences in performing these job demands, as well as the personality characteristics and other factors that contribute to these stress experiences, are not well understood by scholars and may not be readily approached given the relatively nascent and disjoint nature of the applicable stress research to date.

This review synthesized the extant stress research in IS and considered its applicability to cybersecurity professionals to aid scholars in gaining a better understanding of stress within the cybersecurity profession. Overall, our review indicated that the applicable stress research is limited but progressing, and its direct application to cybersecurity professionals needs some contextualization and clarity. As presented in this review, several opportunities exist to extend stress research into the cybersecurity profession.

As this review indicated, security demands imposed on cybersecurity professionals, which are a source of challenge and hindrance stress, should be contextualized from technical and nontechnical perspectives. When contextualizing stress research for cybersecurity professionals, a fundamental limitation was found when delineating the appraisal of demands. In this direction, we pointed out that a demand can have a positive (challenge) appraisal or negative (hindrance) appraisal, the appraisal processes which are the result of an interplay between the characteristics of the cybersecurity professionals apprising a demand and the organizational environment within which demand is being placed. Our future research questions suggest directions in understanding psychological stress, its relationship to the individual (such as personality), and organizational factors (such as InfoSec policies and procedures) constituting the challenge and hindrance stress among cybersecurity professionals. A further elaboration of stress in the cybersecurity profession requires a holistic approach comprising both positive and negative sides, emphasizing that stress is a dual process phenomenon that does not always lead to adverse outcomes and we encourage taking a multidisciplinary approach that draws from and informs the IS, management, organizational behavior and psychology literature.

Although the research opportunities presented in this review are not exhaustive, tackling the challenge of understanding the stress phenomenon among cybersecurity professionals has practical ramifications that extend beyond the research communities. First, as the source of stress is understood, necessary steps can be taken to mitigate the concerning levels of stress and burnout (Winder, 2022; Hinchy, 2022) while improving job satisfaction and work performance among cybersecurity professionals. As new security demands relating to the

challenge and hindrance aspects of stress among cybersecurity professionals come to light, new ways to promote the positive aspects of stress and mitigate the negative side also appear.

5.1 Implications for research and practice

This literature review provides several contributions for academicians as well as practitioners seeking ways to better understand and support the cybersecurity profession. First, by its very nature, this review highlights an omission in the research on stress, namely, research into the phenomenon of stress within the cybersecurity profession. Second, this literature review provides scholars with an explicit set of opportunities for future research on stress in the cybersecurity profession, not currently espoused directly in the extant stress literature. The current lack of focus on stress among the cybersecurity profession underscores a general lack of concern for mental health within the profession; a gap in great need of attention by both academics and professionals that serve to support and grow the profession.

In terms of contributions to practice, this review underscores some of the stressful circumstances cybersecurity professionals face and must cope with in their daily professional lives. This literature review can also benefit cybersecurity professionals, managers and administrators in several ways. First, managers and administrators should pay close attention to the security demands and associated stress levels that cybersecurity professionals are exposed to. Since individual differences affect a demand appraisal process, not every cybersecurity professional will experience the same stress level; some may be more stressed than others and may exhibit different psychological and physiological stress levels. The deteriorating (mental) health of cybersecurity professionals affects their performance and may jeopardize the organization's security. This review identifies several security demands, associated stress responses and stress-related outcomes. Some of those stress responses and outcomes can be more visible than the others, such as an effect on job performance, decision quality, ability to respond to a threat promptly or even desire to quit the job or leave the cybersecurity profession altogether. If the signs are apparent, an open and collaborative approach should be taken to discuss the issues and resources, such as counseling, mentoring, clinical care, etc., should be made available so cybersecurity professionals can engage in their jobs in positive, problem-focused manner.

Another area that organizations should be mindful of is that cybersecurity professionals encounter constantly evolving and changing security threats, so there is unpredictability in the job tasks. Also, as businesses gear up their digital transformation in order to deal with unforeseen and unpredictable factors, they often adopt new operational models, such as remote work during a natural disaster (such as a pandemic), which further worsens the mental health and overall well-being of cybersecurity professionals (Winder, 2022). Although an organization's sponsored employee wellness programs have a positive impact on employee health, long-term efforts for cybersecurity professionals' well-being should be directed toward providing more control over their jobs to address more stressful objectives. Positive stress responses can be anticipated by providing flexible work schedules, which aid in attaining work-life balance through accomplishing family responsibilities and obligations, higher education, professional competencies and personal hobbies.

Lastly, cybersecurity, as a profession, has a persistently high job turnover rate (Wolff, 2019). For instance, Chief Information Security Officers (CISOs) and others in comparable high-ranking positions frequently quit their employment after only 2.5 years, whereas those in lower-level technical positions typically do so after roughly four years (Ponemon, 2014). These turnover rates are even more concerning when combined with the existing cybersecurity workforce gap (HBR, 2019). So, it becomes even more important for organizations to retain the existing talent and direct employee retention efforts through a

mechanism such as a reward, appreciation, recognition and acknowledgment of the critical work they do (Ishmael and Halawi, 2022).

6. Limitations

Although we followed a systematic review process established by Okoli and Schabram (2010) and Okoli (2015), there are some limitations of the process that affected both the scope of the review and, ultimately, the inferences we are able to draw from it. First, this method offers no explicit instructions on how to assess the quality of the research papers to be included in the review, except for the suggestion that the studies should be similar or homogenous in methodological quality so as to draw meaningful conclusions. Such an approach leaves the quality judgment to the discretion of the authors and limits the contribution and reproducibility of the research if the criteria for quality determinations are not explicitly mentioned. Second, if the guidance from Okoli and Schabram (2010) is strictly followed, then it may exclude research based on poor methodological quality and add selection bias. Hence we relied on the inclusion criteria from prior IS stress research (Tarafdar *et al.*, 2019) but acknowledge that our inferences may be consequently limited. For example, although the present review can effectively identify important gaps in the literature, the failure to identify and exclude potentially misleading or insufficiently robust research may lead to the false conclusion that some topics have been addressed even though there remains a need for additional high-quality research.

7. Conclusion

Given the dearth of research on the role of stress among cybersecurity professionals, in this study, we set out to identify what we do know and what might be some valuable new areas of study on this phenomenon. To achieve this goal, it is important to first understand how stress has been approached by IS scholars in their research on cybersecurity and stress phenomena. We used an eight-step systematic literature review process to identify the gaps and trends in the extant research and illuminate potentially valuable paths for future research (Okoli, 2015; Okoli and Schabram, 2010). We contend that the existing general workplace and IS-specific stress literature can contribute to the research of stress experiences among cybersecurity professionals. In the end, this review provides actionable recommendations for future research into stress among cybersecurity professionals.

Notes

1. Demands are the events or the characteristics or properties of events that individuals encounter (Kahn and Byosiere, 1992). Once demands are appraised, they are termed as "stressors" in this review.

References

Aggarwal, A. and Dhurkari, R.K. (2023), "Association between stress and information security policy non-compliance behavior: a meta-analysis", *Computers and Security*, Vol. 124, p. 102991.

Ahuja, M.K., Chudoba, K.M., Kacmar, C.J., Mcknight, D.H. and George, J.F. (2007), "IT road warriors: balancing work-family conflict, job autonomy, and work overload to mitigate turnover intentions", *MIS Quarterly*, Vol. 31, pp. 1-17.

Ament, C. and Haag, S. (2016a), "How information security requirements stress employees", *International Conference on Information Systems (ICIS)*, Dublin.

Ament, C. and Haag, S. (2016b), "Security-related stress-a neglected contruct in information systems stress literature", *European Conference on Information Systesm (ECIS)*, İstanbul.

Anderson, B.B., Vance, A., Kirwan, C.B., Eargle, D. and Jenkins, J.L. (2016), "How users perceive and respond to security messages: a NeuroIS research agenda and empirical study", *European Journal of Information Systems*, Vol. 25, pp. 364-390.

Armstrong, D.J., Brooks, N.G. and Riemenschneider, C.K. (2015), "Exhaustion from information system career experience: implications for turn-away intention", *MIS Quarterly*, Vol. 39, pp. 713-728.

Ayyagari, R., Grover, V. and Purvis, R. (2011), "Technostress: technological antecedents and implications", *MIS Quarterly*, Vol. 35, pp. 831-858.

Bashir, M., Lambert, A., Wee, J.M.C. and Guo, B. (2015), "An examination of the vocational and psychological characteristics of cybersecurity competition participants", *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Bashir, M., Wee, C., Memon, N. and Guo, B. (2017), "Profiling cybersecurity competition participants: self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool", *Computers and Security*, Vol. 65, pp. 153-165.

Beaudry, A. and Pinsonneault, A. (2005), "Understanding user responses to information technology: a coping model of user adaptation", *MIS Quarterly*, Vol. 29, pp. 493-524.

Beaudry, A. and Pinsonneault, A. (2010), "The other side of acceptance: studying the direct and indirect effects of emotions on information technology use", *MIS Quarterly*, Vol. 34, pp. 689-710.

Brody, B.A. (2019), *Cybersecurity Akin to Being in a War Zone—You Have to be "Left of Boom" to Survive*, ISACA Now Blog, available at: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=520&utm_referrer=direct%2Fnot%20provided (accessed 25 October 2019).

Bryant, F.B. and Veroff, J. (2007), *Savoring: A New Model of Positive Experience*, Lawrence Erlbaum Associates, Mahwah, NJ.

Budnick, C.J., Rogers, A.P. and Barber, L.K. (2020), "The fear of missing out at work: examining costs and benefits to employee health and motivation", *Computers in Human Behavior*, Vol. 104, p. 106161.

Califf, C.B., Sarker, S. and Sarker, S. (2020), "The bright and Dark sides of technostress: a mixed-methods study involving Healthcare IT", *MIS Quarterly*, Vol. 44, pp. 809-856.

Cavanaugh, M.A., Boswell, W.R., Roehling, M.V. and Boudreau, J.W. (2000), "An empirical examination of self-reported work stress among US managers", *Journal of Applied Psychology*, Vol. 85, pp. 65-74.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2005), "The value of intrusion detection systems in information technology security architecture", *Information Systems Research*, Vol. 16, pp. 28-46.

Chen, A. and Karahanna, E. (2018), "Life interrupted: the effects of technology-mediated work interruptions on work and nonwork outcomes", *MIS Quarterly*, Vol. 42, pp. 1023-1042.

Chilton, M.A., Hardgrave, B.C. and Armstrong, D.J. (2005), "Person-job cognitive style fit for software developers: the effect on strain and performance", *Journal of Management Information Systems*, Vol. 22, pp. 193-226.

Cobb, S. (2016), "Mind this gap: criminal hacking and the global cybersecurity skills shortage, a critical analysis", *Virus Bulletin Conference*, Denver, CO.

Cooper, C.L., Dewe, P.J. and O'driscoll, M.P. (2001), *Organizational Stress: A Review and Critique of Theory, Research, and Applications*, Sage, Thousand Oaks, CA.

Crossler, R.E., Di Gangi, P.M., Johnston, A.C., Bélanger, F. and Warkentin, M. (2018), "Providing theoretical foundations: developing an integrated set of guidelines for theory adaptation", *Communications of the Association for Information Systems*, Vol. 43, pp. 566-597.

D'arcy, J. and Teh, P.-L. (2019), "Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization", *Information and Management*, Vol. 56, p. 103151.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31, pp. 285-318.

D'Arcy, J., Herath, T., Yim, M.-S., Nam, K. and Rao, H.R. (2018), "Employee moral disengagement in response to stressful information security requirements: a methodological replication of a coping-based model", *AIS Transactions on Replication Research*, Vol. 4, pp. 1-18.

Deep Instinct (2022), "Why your cybersecurity leaders and staff are thinking about leaving", available at: https://www.deepinstinct.com/pdf/voice-of-secops-3rd-edition-infographic (accessed 20 November 2022).

Dimoka, A., Pavlou, P.A. and Davis, F.D. (2011), "Research commentary: NeuroIS: the potential of cognitive neuroscience for information systems research", *Information Systems Research*, Vol. 22, pp. 687-702.

Edwards, J.R. (1992), "A cybernetic theory of stress, coping, and well-being in organizations", *Academy of Management Review*, Vol. 17, pp. 238-274.

Edwards, J.R. (1996), "An examination of competing versions of the person-environment fit approach to stress", *Academy of Management Journal*, Vol. 39, pp. 292-339.

Edwards, J.A. and Billsberry, J. (2010), "Testing a multidimensional theory of person-environment fit", *Journal of Managerial Issues*, Vol. 22, pp. 476-493.

Edwards, J.R. and Cooper, C.L. (1990), "The person-environment fit approach to stress: recurring problems and some suggested solutions", *Journal of Organizational Behavior*, Vol. 11, pp. 293-307.

Fadel, K.J. (2012), "User adaptation and infusion of information systems", *Journal of Computer Information Systems*, Vol. 52, pp. 1-10.

Fischer, T. and Riedl, R. (2017), "Technostress research: a nurturing ground for measurement pluralism?", *Communications of the Association for Information Systems*, Vol. 40, p. 17.

Folkman, S. and Lazarus, R.S. (1985), "If it changes it must be a process: study of emotion and coping during three stages of a college examination", *Journal of Personality and Social Psychology*, Vol. 48, pp. 150-170.

Fuglseth, A.M. and Sørebø, Ø. (2014), "The effects of technostress within the context of employee use of ICT", *Computers in Human Behavior*, Vol. 40, pp. 161-170.

Galluch, P.S., Grover, V. and Thatcher, J.B. (2015), "Interrupting the workplace: examining stressors in an information technology context", *Journal of the Association for Information Systems*, Vol. 16, pp. 1-47.

George, J.F. (1996), "Computer-based monitoring: common perceptions and empirical results", *MIS Quarterly*, Vol. 20, pp. 459-480.

Hargrove, M.B., Nelson, D.L. and Cooper, C.L. (2013), "Generating eustress by challenging employees: helping people savor their work", *Organizational Dynamics*, Vol. 42, pp. 61-69.

Hargrove, M.B., Becker, W.S. and Hargrove, D.F. (2015), "The HRD eustress model: generating positive stress with challenging work", *Human Resource Development Review*, Vol. 14, pp. 279-298.

Harms, P.D., Krasikova, D.V., Vanhove, A.J., Herian, M.N. and Lester, P.B. (2013), *Stress and Emotional Well-Being in Military Organizations. The Role of Emotion and Emotion Regulation in Job Stress and Well Being*, Emerald Group Publishing, Bingley.

HBR (2019), *The Public-Private Partnership That's Working to Make New York City a Global Hub of Cybersecurity Talent*, Harvard Business Review, available at: https://hbr.org/sponsored/2019/06/the-public-private-partnership-thats-working-to-make-new-york-city-a-global-hub-of-cybersecurity-talent (accessed 26 April 2021).

Helkala, K., Knox, B., Jøsok, Ø., Knox, S. and Lund, M. (2016), "Factors to affect improvement in cyber officer performance", *Information and Computer Security*, Vol. 24, pp. 152-163.

Hinchy, E. (2022), *State of Mental Health in Cybersecurity*, Tines. Com, available at: https://www.tines.com/reports/state-of-mental-health-in-cybersecurity/ (accessed 11 November 2022).

Hwang, I. and Cha, O. (2018), "Examining technostress creators and role stress as potential threats to employees' information security compliance", *Computers in Human Behavior*, Vol. 81, pp. 282-293.

Hwang, I., Kim, S. and Rebman, C. (2021), "Impact of regulatory focus on security technostress and organizational outcomes: the moderating effect of security technostress inhibitors", *Information Technology and People*, Vol. 35 No. 7, pp. 2043-2074.

IBM (2022), "IBM security incident responder study", available at: https://www.ibm.com/downloads/cas/XKOY5OLO (accessed 19 November 2022).

Igbaria, M. and Guimaraes, T. (1993), "Antecedents and consequences of job satisfaction among information center employees", *Journal of Management Information Systems*, Vol. 9, pp. 145-174.

Igbaria, M., Parasuraman, S. and Badawy, M.K. (1994), "Work experiences, job involvement, and quality of work life among information systems personnel", *MIS Quarterly*, Vol. 18, pp. 175-201.

$(ISC)^2$ (2018), "Cybersecurity professionals focus on developing new skills as workforce gap widens", $(ISC)^2$, Cybersecurity Workforce Study, 2018, available at: https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx (accessed 25 October 2019).

Ishmael, A. and Halawi, D.L. (2022), "Retention of qualified cybersecurity professionals: a qualitative study", *Journal of Computer Information Systems*, Vol. 63 No. 1, pp. 204-215.

Jensen, M.L., Dinger, M., Wright, R.T. and Thatcher, J.B. (2017), "Training to mitigate phishing attacks using mindfulness techniques", *Journal of Management Information Systems*, Vol. 34, pp. 597-626.

Johnston, A.C., Di Gangi, P.M., Howard, J. and Worrell, J. (2019), "It takes a village: understanding the collective security efficacy of employee groups", *Journal of the Association for Information Systems*, Vol. 20, pp. 186-212.

Joseph, D., Ng, K.-Y., Koh, C. and Ang, S. (2007), "Turnover of information technology professionals: a narrative review, meta-analytic structural equation modeling, and model development", *MIS Quarterly*, Vol. 31, pp. 547-577.

Kahn, R.L. and Byosiere, P. (1992), *Stress in Organizations, Handbook of Industrial and Organizational Psychology*, Consulting Psychologists Press, Palo Alto, CA.

Karasek, R.A. Jr (1979), "Job demands, job decision latitude, and mental strain: implications for job redesign", *Administrative Science Quarterly*, Vol. 24, pp. 285-308.

Krishnan, S. (2017), "Personality and espoused cultural differences in technostress creators", *Computers in Human Behavior*, Vol. 66, pp. 154-167.

Kropotov, V. and Yarochkin, F. (2019), "How social media can be used to gather intelligence", available at: https://www.trendmicro.com/vinfo/it/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter (accessed 11 November 2022).

Lazarus, R.S. and Folkman, S. (1984), *Stress, Appraisal, and Coping*, Springer Publishing, New York.

Lazarus, R.S. and Folkman, S. (1987), "Transactional theory and research on emotions and coping", *European Journal of Personality*, Vol. 1, pp. 141-169.

Lee, C., Lee, C.C. and Kim, S. (2016), "Understanding information security stress: focusing on the type of information security compliance activity", *Computers Security*, Vol. 59, pp. 60-70.

LePine, J.A., Lepine, M.A. and Jackson, C.L. (2004), "Challenge and hindrance stress: relationships with exhaustion, motivation to learn, and learning performance", *Journal of Applied Psychology*, Vol. 89, pp. 883-891.

LePine, J.A., Podsakoff, N.P. and Lepine, M.A. (2005), "A meta-analytic test of the challenge stressor–hindrance stressor framework: an explanation for inconsistent relationships among stressors and performance", *Academy of Management Journal*, Vol. 48, pp. 764-775.

LePine, M.A., Zhang, Y., Crawford, E.R. and Rich, B.L. (2016), "Turning their pain to gain: charismatic leader influence on follower stress appraisal and job performance", *Academy of Management Journal*, Vol. 59, pp. 1036-1059.

Lerouge, C., Nelson, A. and Blanton, J.E. (2006), "The impact of role stress fit and self-esteem on the job attitudes of IT professionals", *Information and Management*, Vol. 43, pp. 928-938.

Li, E.Y. and Shani, A.B. (1991), "Stress dynamics of information systems managers: a contingency model", *Journal of Management Information Systems*, Vol. 7, pp. 107-130.

Liang, H. and Xue, Y. (2009), "Avoidance of information technology threats: a theoretical perspective", *MIS Quarterly*, Vol. 33, pp. 71-90.

Liang, H., Xue, Y., Pinsonneault, A. and Wu "Andy", Y. (2019), "What users do besides problem-focused coping when facing IT security threats: an emotion-focused coping perspective", *MIS Quarterly*, Vol. 43, pp. 373-394.

Louie, R. (2018), "Cybersecurity impact on mental health: managing stress, building resilience", *RSA Conference 2018*, available at: https://www.rsaconference.com/usa/us-2018/agenda/cybersecurity-impact-on-mental-health-managing-stress-building-resilience (accessed 2 February 2020).

Maier, C., Wirth, J., Laumer, S. and Weitzel, T. (2017), "Personality and technostress: theorizing the influence of IT mindfulness", *International Conference on Information Systems (ICIS), Seoul.*

Maier, C., Laumer, S., Wirth, J. and Weitzel, T. (2019), "Technostress and the hierarchical levels of personality: a two-wave study with multiple data samples", *European Journal of Information Systems*, Vol. 28, pp. 496-522.

Maslach, C. and Jackson, S.E. (1981), "The measurement of experienced burnout", *Journal of Organizational Behavior*, Vol. 2, pp. 99-113.

Maslach, C. and Jackson, S.E. (1986), *Maslach Burnout Inventory*, Consulting Psychologists Press, Palo Alto, CA.

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M. and Lillie, M. (2018), "The effect of resilience and job stress on information security awareness", *Information and Computer Security*, Vol. 26, pp. 277-289.

McGrath, J.E. (1970), "A conceptual formulation for research on stress", in McGrath, J.E. (Ed.), *Social and Psychological Factors in Stress*, Holt Rinehart, & Winston, New York.

McGrath, J.E. (1976), "Stress and behavior in organizations", in Dunnette, M.D. (Ed.), *Handbook of Industrial and Organizational Psychology*, Rand McNally, Chicago.

Monica, A. and Gloria, P.-W. (2019), "Stressed decision makers and use of decision aids: a literature review and conceptual model", *Information Technology and People*, Vol. 33, pp. 710-754.

Moody, G.D. and Galletta, D.F. (2015), "Lost in Cyberspace: the impact of information scent and time constraints on stress, performance, and attitudes online", *Journal of Management Information Systems*, Vol. 32, pp. 192-224.

Moore, J.E. (2000), "One road to turnover: an examination of work exhaustion in technology professionals", *MIS Quarterly*, Vol. 24, pp. 141-168.

Nasirpouri Shadbad, F. and Biros, D. (2021), "Understanding employee information security policy compliance from role theory perspective", *Journal of Computer Information Systems*, pp. 1-10.

Okoli, C. (2015), "A guide to conducting a standalone systematic literature review", *Communications of the Association for Information Systems*, Vol. 37, pp. 879-910.

Okoli, C. and Schabram, K. (2010), "A guide to conducting a systematic literature review of information systems research", *Communications of the Association for Information Systems*, Vol. 37, pp. 879-910.

Olmstead, K., Lampe, C. and Ellison, N.B. (2016), *Social Media and the Workplace*, Pew Research Center, available at: https://www.pewresearch.org/internet/2016/06/22/social-media-and-the-workplace/ (accessed 11 November 2022).

Oltsik, J. (2019), "The most stressful aspects of being a cybersecurity professional", available at: https://www.csoonline.com/article/3395865/the-most-stressful-aspects-of-being-a-cybersecurity-professional.html (accessed 25 October 2019).

Oltsik, J. and Alexander, C. (2018), "The life and times of cybersecurity professionals", available at: https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf (accessed 2 February 2020).

Pfleeger, C.P. and Pfleeger, S.L. (2012), *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*, Prentice Hall Professional.

Pham, H.C. (2019), "Information security burnout: identification of sources and mitigating factors from security demands and resources", *Journal of Information Security Applications*, Vol. 46, pp. 96-107.

Pham, H.-C., El-Den, J. and Richardson, J. (2016), "Stress-based security compliance model – an exploratory study", *Information and Computer Security*, Vol. 24, p. 326.

Pirkkalainen, H., Salo, M., Tarafdar, M. and Makkonen, M. (2019), "Deliberate or instinctive? Proactive and reactive coping for technostress", *Journal of Management Information Systems*, Vol. 36, pp. 1179-1212.

Podsakoff, N.P., Lepine, J.A. and Lepine, M.A. (2007), "Differential challenge stressor-hindrance stressor relationships with job attitudes, turnover intentions, turnover, and withdrawal behavior: a meta-analysis", *Journal of Applied Psychology*, Vol. 92, pp. 438-454.

Ponemon (2014), "Understaffed and at risk: today's IT security department", available at: https://www.ponemon.org/local/upload/file/IT%20Security%20Jobs%20Research%20Report%20FINAL4.pdf (accessed 2 February 2020).

Posey, C., Bennett, B., Roberts, T. and Lowry, P.B. (2011), "When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse", *Journal of Information Systems Security*, Vol. 7, pp. 24-47.

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

Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B.S. and Tu, Q. (2008), "The consequences of technostress for end users in organizations: conceptual development and empirical validation", *Information Systems Research*, Vol. 19, pp. 417-433.

Riedl, R., Davis, F.D. and Hevner, A.R. (2014), "Towards a NeuroIS research methodology: intensifying the discussion on methods, tools, and measurement", *Journal of the Association for Information Systems*, Vol. 15, pp. i-xxxv.

Rutner, P.S., Hardgrave, B.C. and Mcknight, D.H. (2008), "Emotional dissonance and the information technology professional", *MIS Quarterly*, Vol. 32, pp. 635-652.

Shih, S.-P., Jiang, J.J., Klein, G. and Wang, E. (2011), "Learning demand and job autonomy of IT personnel: impact on turnover intention", *Computers in Human Behavior*, Vol. 27, pp. 2301-2307.

Shih, S.-P., Jiang, J.J., Klein, G. and Wang, E. (2013), "Job burnout of the information technology worker: work exhaustion, depersonalization, and personal accomplishment", *Information and Management*, Vol. 50, pp. 582-589.

Shropshire, J. and Kadlec, C. (2012), "I'm leaving the IT field: the impact of stress, job insecurity, and burnout on IT professionals", *International Journal of Information and Communication Technology Research*, Vol. 2, pp. 6-16.

Simmons, B.L. and Nelson, D.L. (2001), "Eustress at work: the relationship between hope and health in hospital nurses", *Health Care Management Review*, Vol. 26, pp. 7-18.

Simmons, B.L. and Nelson, D.L. (2007), "Eustress at work: extending the holistic stress model", in Nelson, D.L. and Cooper, C.L. (Eds), *Positive Organizational Behavior*, Sage, London.

Sonnentag, S. and Frese, M. (2003), "Stress in organizations", in *Handbook of Psychology*, pp. 453-491.

Srivastava, S.C., Chandra, S. and Shirish, A. (2015), "Technostress creators and job outcomes: theorising the moderating influence of personality traits", *Information Systems Journal*, Vol. 25, pp. 355-401.

Stich, J.-F., Tarafdar, M., Stacey, P. and Cooper, C.L. (2019a), "E-mail load, workload stress and desired e-mail load: a cybernetic approach", *Information Technology and People*, Vol. 32, pp. 430-452.

Stich, J.-F., Tarafdar, M., Stacey, P. and Cooper, S.C. (2019b), "Appraisal of email use as A source of workplace stress: a person-environment fit approach", *Journal of the Association for Information Systems*, Vol. 20, pp. 132-160.

Tams, S., Ahuja, M., Thatcher, J. and Grover, V. (2020), "Worker stress in the age of mobile technology: the combined effects of perceived interruption overload and worker control", *The Journal of Strategic Information Systems*, Vol. 29, p. 101595.

Tams, S., Grover, V., Thatcher, J. and Ahuja, M. (2017), "When modern technologies meet ageing workforces: older workers are more affected by demands from mobile interruptions than their younger counterparts", *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hawaii.

Tams, S., Hill, K., De Guinea, A.O., Thatcher, J. and Grover, V. (2014), "NeuroIS—alternative or complement to existing methods? Illustrating the holistic effects of neuroscience and self-reported data in the context of technostress research", *Journal of the Association for Information Systems*, Vol. 15, pp. 723-753.

Tams, S., Legoux, R. and Léger, P.-M. (2018a), "Smartphone withdrawal creates stress: a moderated mediation model of nomophobia, social threat, and phone withdrawal context", *Computers in Human Behavior*, Vol. 81, pp. 1-9.

Tams, S., Thatcher, J.B. and Grover, V. (2018b), "Concentration, competence, confidence, and capture: an experimental study of age, interruption-based technostress, and task performance", *Journal of the Association for Information Systems*, Vol. 19, pp. 857-908.

Tarafdar, M., Cooper, C.L. and Stich, J.F. (2019), "The technostress trifecta-techno eustress, techno distress and design: theoretical directions and an agenda for research", *Information Systems Journal*, Vol. 29, pp. 6-42.

Tarafdar, M., Gupta, A. and Turel, O. (2015), "Introduction to the special issue on 'Dark side of information technology use'–Part two", *Information Systems Journal*, Vol. 25, pp. 315-317.

Tarafdar, M., Tu, Q., Ragu-Nathan, B.S. and Ragu-Nathan, T. (2007), "The impact of technostress on role stress and productivity", *Journal of Management Information Systems*, Vol. 24, pp. 301-328.

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

Trang, S. and Nastjuk, I. (2021), "Examining the role of stress and information security policy design in information security compliance behaviour: an experimental study of in-task behaviour", *Computers and Security*, Vol. 104, p. 102222.

Vance, A., Anderson, B.B., Kirwan, C.B. and Eargle, D. (2014), "Using measures of risk perception to predict information security behavior: insights from electroencephalography (EEG)", *Journal of the Association for Information Systems*, Vol. 15, pp. 679-722.

Venkatesh, V., Rai, A. and Maruping, L.M. (2018), "Information systems projects and individual developer outcomes: role of project managers and process control", *Information Systems Research*, Vol. 29, pp. 127-148.

Vogel, R. (2016), "Closing the cybersecurity skills gap", *Salus Journal*, Vol. 4, pp. 32-46.

Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R. and Cleven, A. (2015), "Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research", *Communications of the Association for Information Systems*, Vol. 37, pp. 205-224.

Wang, K., Shu, Q. and Tu, Q. (2008), "Technostress under different organizational environments: an empirical investigation", *Computers in Human Behavior*, Vol. 24, pp. 3002-3013.

Wang, J., Li, Y. and Rao, H.R. (2017), "Coping responses in phishing detection: an investigation of antecedents and consequences", *Information Systems Research*, Vol. 28, pp. 378-396.

Wang, X., Tan, S.C. and Li, L. (2020), "Technostress in university students' technology-enhanced learning: an investigation from multidimensional person-environment misfit", *Computers in Human Behavior*, Vol. 105, p. 106208.

Warkentin, M., Walden, E., Johnston, A.C. and Straub, D.W. (2016), "Neural correlates of protection motivation for secure IT behaviors: an fMRI examination", *Journal of the Association for Information Systems*, Vol. 17, pp. 194-215.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MIS Quarterly*, Vol. 26, pp. 13-23.

Windeler, J.B., Maruping, L. and Venkatesh, V. (2017), "Technical systems development risk factors: the role of empowering leadership in lowering developers' stress", *Information Systems Research*, Vol. 28, pp. 775-796.

Winder, D. (2022), *Mental Health in Cybersecurity—51% of Workers Take Meds, Me Included*, Forbes.com, available at: https://www.forbes.com/sites/daveywinder/2022/06/08/mental-health-in-cybersecurity-51-of-workers-take-meds-me-included/?sh=17315e86573a (accessed 11 November 2022).

Wolff, J. (2019), "Cybersecurity experts are leaving the federal government. That's a problem", *International New York Times*, available at: https://link.gale.com/apps/doc/A609461957/GIC?u=tusc49521&sid=GIC&xid=fb0172e3 (accessed 11 November 2021).

Yu, L., Cao, X., Liu, Z. and Wang, J. (2018), "Excessive social media use at work: exploring the effects of social media overload on job performance", *Information Technology and People*, Vol. 31, pp. 1091-1112.

Zhao, X., Xia, Q. and Huang, W. (2020), "Impact of technostress on productivity from the theoretical perspective of appraisal and coping processes", *Information and Management*, Vol. 57, p. 103265.

Zurkus, K. (2019), "Dispelling the 'security as bad guy' myth", available at: https://securityboulevard.com/2019/02/dispelling-the-security-as-bad-guy-myth/ (accessed 5 May 2021).

Appendix

The supplementary material for this article can be found online.

Corresponding author

Tripti Singh can be contacted at: triptis@mtu.edu