HOLISTICA Vol 13, Issue 1, 2022, pp. 49-72 DOI:10.2478/hjbpa-2022-0003

STRESS, BURNOUT, AND SECURITY FATIGUE IN CYBERSECURITY: A HUMAN FACTORS PROBLEM

Calvin NOBLES[1]

Received: January 2022 |Accepted: April 2022 | Published: July 2022
Please cite this paper as: Nobles, C. (2022) Stress, burnout and security fatigue in cybersecurity: A human factors problem, *Holistica Journal of Business and Public Administration*, Vol. 13, Iss. 1, pp. 49-72

Abstract

Stress, burnout, and security fatigue continue as slight destroyers of strong cybersecurity and significant human factors concerns. The persistence of these human performance issues is concerning given the lack of mitigation and integration of human factors practitioners to mitigate these adverse risk circumstances. Security fatigue is not a new phenomenon but the evolving nature of cybersecurity results in various sub-categories of security fatigue; thus, making it a difficult problem to solve. Stress and burnout are major causes of short tenures in senior roles for security executives. Business decision-makers lack the expertise to explore the negative influences of stress, burnout, and security fatigue on cybersecurity. Technology-led cycles are organizations' primary course of action to mitigate cybersecurity threats, resulting in complexity debt and making businesses more vulnerable to attacks. Human factors professionals can identify high-friction areas that degrade human performance and implement initiatives to reduce the risk. Human performance degradation in cybersecurity is a critical risk factor and requires immediate attention, given that cybercriminals continue to exploit human weaknesses to gain access to sensitive and critical infrastructure.

Keywords: Complexity Debt, Cybersecurity, Behavior, Burnout, Fatigue, Human Factors, Human Performance, Security Fatigue, and Stress

1. Introduction

An existing phenomenon that continues to plague information security and cybersecurity is fatigue and burnout. Recently, the topic of job burnout has been trending in several practitioner-based security magazines, blogs, social media, and websites (Platsis, 2019). In addition, a recent study by a reputable university in the U.K. and a security vendor highlighted the pervasive nature of cybersecurity burnout and its implications on businesses, individuals, and the industry (Platsis, 2019). One researcher indicated that the technological pace, operational demands, and relentless threats

[1] *Illinois Institute of Technology, Cybersecurity Fellow, Harvard University Belfer Center, USA, Cnobles1@iit.edu*

coupled with disjointed security capabilities and non-integrated products contribute to job burnout in the cybersecurity domain (Platsis, 2019).

Stress, burnout, and cybersecurity fatigue issues are not new to cybersecurity; however, the occurrences and consequences are mounting due to business decision-makers (BDM), primarily senior management, failure to address the root causes of stress, burnout, and fatigue. Researchers noted that security practitioners are overtaxed, stressed out, and inaccessible (Dykstra & Paul, 2018); hence, leading to the shortage of scientific research on security fatigue. Operational stress, fatigue, error, and burnout are extensively documented in the literature (Grier, 2015); however, fatigue in cybersecurity remains less than a top-tier discussion topic for security and technology executives. Grier (2015) indicated that other sociotechnical fields such as aviation, industrial control and command, and medicine had investigated workload because these fields mandate high cognitive skills, awareness, memory, and visual perception abilities. The significance of studying workload and stress is the scientifically proven correlation of errors and decreased performance (Dykstra & Paul, 2018; Nobles, 2019). A study by Dykstra and Paul (2018), who examined cyber operators, revealed that operation fatigue and frustration increased throughout the length of the cyber operation

Nobles (2019) postulated that organizations and BDM have not thoroughly explored the issues causing security fatigue. The three pillars of information security are (a) people, (b) technology, and (c) processes. Failure to address security fatigue in cybersecurity resulted in upticks in data breaches, cyber-attacks, ransomware attacks, and other security catastrophes. Existing research indicates that 80-90% of security incidents stem from human errors in the U.S. and the U.K. (Nobles, 2018). The dynamic nature of the business environment, coupled with increased reliance on advanced technologies, a shortage of cybersecurity, increased regulatory demands, and a relentless cybersecurity threat landscape, perpetuates security fatigue (Nobles, 2019). This paper aims to instigate discourse, empirical research, and operational practices to address the root causes of stress, security fatigue, and burnout in cybersecurity. Another objective of this article is to highlight the critical need to address security fatigue in cybersecurity operations due to increased risk.

2. Background

A recent survey divulged that Chief Information Security Officers (CISO) are overworked, impacting their mental health to the degree that 90% are willing to take a pay cut (Sheridan, 2020). The continuous stress and mental health implications disrupt the CISOs work-life balance; 88% of the executive were overly stressed (Sheridan, 2020). The survey did not list the factors for inducing the pressure (Sheridan, 2020). ISACA indicates that CISOs are responsible for a myriad of responsibilities, leading to too much strain and stress (ISACA, 2020). The grueling nature of the CISO position results in short tenures from 1 to 2 years due to the increasing responsibility, less personal and recovery time, and the constant connectivity (ISACA, 2020). The demanding responsibilities

placed on CISOs and security professionals lead to mental health concerns and unprecedented stress levels (ISACA, 2020; Sheridan, 2020). At issue is the increased stress levels and the potential to cascade throughout the ranks of the security team; consequently, possibly resulting in burnout and chronic fatigue.

Chief Information Security Officers are not the only individuals impacted by security fatigue. For example, a National Institute of Standards and Technology study indicated that people engaged in risky behavior while working and at home (Stanton, Theofanos, Prettyman, & Furman, 2016). In addition, the study discovered that workers are overwhelmed while interacting with computer systems due to experiencing substandard security experiences, resulting in security fatigue and degraded security decision-making (Stanton, Theofanos, Prettyman, & Furman, 2016). This growing phenomenon of security lethargicness requires immediate remediation and solutions because cybercriminals continuously attack employees' cognitive abilities. In addition, cybercriminals leverage deceptive practices to target humans to provide sensitive, personal, or private information to steal their login credentials and illegally gain access to computer networks (Bone, 2017). Failure to address human performance issues in cybersecurity or interacting with information systems will continue to allow cybercriminals to continuously execute malicious activity detrimental to business organizations and people.

People perform countless security tasks daily privately and professionally; consequently, these tasks require physical and cognitive abilities, which takes a toll on individuals, especially if the security functions are deemed excessive, illogical, or impractical to the users (Parker, Krol, Becker, & Sasse, 2016). Researchers emphasized that security compliance and the burdensome of constant security tasks can exceed an individual's physical and cognitive abilities, resulting in security fatigue (Parker et al., 2016). Pfleeger et al. (2014) stressed that security tasks deplete employees' energy reservoir, especially with cognitively demanding security functions (Parker et al., 2016). Renaud (2012) stated that organizations' security policies place impractical requirements on workers. The abovementioned suppositions highlight the lack of human factors strategies and initiatives in cybersecurity. This is primarily because the cybersecurity industry lags in leveraging human factors as a core capability (Nobles, 2019).

3. Cybersecurity Threat Landscape

The current cybersecurity threat landscape remains challenging for organizations. The proliferation of digitalization increases the surface attack areas of private and public organizations. In a detailed report by the European Union Agency for Cybersecurity (*ENISA, 2021),* ransomware attacks were the primary attack vector accompanied by the COVID-19 pandemic acting as catalysts for human errors and system misconfigurations, as indicated by most data breaches stemming from human errors. The cybersecurity threat landscape is plagued with nefarious actions from the following categories of actors: (a) state-sponsored, (b) cybercriminals, (c) hackers-for-hire, and (d) hacktivists

(ENISA, 2021). The monetization of malicious cyber activities increasingly drives cybercriminals, while cryptocurrency remains the universal payout mechanism for cybercrime (ENISA, 2021).

Phishing-as-a-service, ransomware-as-a-service, ransom-denial-of-service, disinformation-as-a-service coupled with artificial intelligence-enabled information, business email compromise (ENISA, 2021), and traditional attack methodologies are increasing the complexity of the cyber threat environment. The significance of human performance and cognition are essential given the increase in human errors such as system misconfigurations.

The integration of digital technologies increases cybercrime, which researchers forecast the cost of global cybercrime to reach 6 trillion dollars in 2021 (Lallie et al., 2021). The cost of global cybercrime increased from 3 trillion dollars in 2015 (Lallie et al., 2021), indicative of a hyperactive cybersecurity threat environment. During COVID-19, researchers noted a mounting increase in online crimes due to organizations leveraging online technologies to support work from home (Okereafor & Adelaiye, 2020). Some of the prominent attack practices leveraged by cybercriminals are (a) phishing with malware, (b) denial of service, (c) ransomware, (d) vishing, (e) smishing, and (f) zero-day exploit, and (g) man-in-the-middle. The upsurge of work from home during COVID-19 forced organizations to leverage cloud infrastructure rapidly; however, the shortage of cloud expertise resulted in a poorly deployed and managed cloud environment, which creates exploitation opportunities for cybercriminals (ENISA, 2021). Without a doubt, COVID-19 exacerbated cyber-attacks as malicious actors capitalized on employees working from home. Social engineering or cognitive hacking is a growing phenomenon that emerged before the pandemic; yet remains a challenge.

3.1 Cognitive Hacking

Cognitive hacking is not a new concept in computer security. For example, Cybenko, Giani, and Thompson (2002) articulated that cognitive hacking pertains to outwitting users to conduct certain behaviors to aid in executing the cognitive attack through perception manipulation. Cybercriminals and hackers continue to exploit end-users psychological limitations and weaknesses because organizations fail to implement risk management solutions to address cognitive attacks (Bone, 2017). Cognitive hacks are either covert or overt; in covert attacks, the attackers attempt to disguise the manipulation, and overt attacks occur in the form of nuisances and bothersome (Cybenko, Giani, &Thompson, 2002). Given that cognitive hacking has been a significant vector to impede cybersecurity programs without any viable solutions is problematic and indicative of the complexity associated with cybercriminals and malicious actors attacking the end-users' psychological limitations.

Research indicates that "cognitive hacking refers to a computer or information system attack that relies on changing human users' perceptions and corresponding behaviors in order to be successful" (Bones, 2017, p. 134). Phishing, vishing, smishing, spear phishing, and social engineering attacks are forms of cognitive hacking. A significant concern for

HPI in cybersecurity is due to the increasing number of cognitive attacks. Stress, fatigue, and burnout reduce the performance capacity of employees, especially business decision-makers and cybersecurity professionals; consequently, enabling cybercriminals and hackers to capitalize on the employees' debilitated state and lack of awareness.

The proliferation of new technology supports cybercriminals with new avenues to attack employees accompanied by high workloads, inattention blindness, complexity, and risk deafness (Bone, 2017). Business decision-makers struggle to understand the human element, specifically, human factors as a scientific discipline. Given that the human factor is largely underexplored in cybersecurity (Hull, 2017; Nobles, 2018), cognitive hacking and the associated risk factors remain in a state of risk deafness (Bone, 2017). One reason for the continual struggle with cognitive hacking is that organizations lack the organic talent to remediate the associated issues (Nobles, 2019). Given the increasing intricacy of cognitive hacking, psychology-based professionals, including human factors practitioners, should be integrated into cybersecurity operations to develop practical solutions.

4. Human Performance Issues in Cybersecurity

Burnout, fatigue, and stress plague cybersecurity operations; these problems existed before COVID-19, and during the pandemic, human performance issues (HPI) in cybersecurity reached unprecedented levels (Nobles, 2021a). Unfortunately, these quandaries are sustained and continue to wreak havoc on cybersecurity efforts with little to no recourse to remediate these problems (Nobles, 2021a). Table 1 provides a definition and examples of each of the HPI.

These issues negatively impact cybersecurity in the form of decreased production, lower cognition, noncompliance, lack of appreciation, low-security awareness, directionlessness, and lethargy. These symptoms counter the effectiveness of your cybersecurity programs. Unfortunately, adverse human performance issues in cybersecurity are largely under-explored and under-researched (Hull, 2017). As a result, cybersecurity professionals and information technologists undergo continuous and demanding changes to include countering determined and sophisticated cybercriminals.

Table 1 Human Performance Issues in Cybersecurity

Human Performance Issues		
Human Performance Factors	**Definition**	**Examples**
Burnout	Burnout is defined as emotional weariness and exhaustion, depersonalization, lacking competence, and detached attitude about your work (Cong Pham et al.,	1. Overload burnout 2. Neglect burnout 3. Under-utilized burnout

	2019; Nori et al., 2019).	
Security Fatigue	Security fatigue is lethargy or reluctance to deal with computer security and compliance due to being overwhelmed or in conflict with one's bounded rationality to acquire and practice effective security behavior (Stanton et al., 2016).	1. Authentication fatigue 2. Compliance fatigue 3. Alert fatigue 4. Decision fatigue 5. Regulatory fatigue
Stress	Stress is a physical and emotional response to specific circumstances….Acute stress is the fight or flight concept in which the symptoms are short-term….while episodic stress pertains to exposure to repeated stressful events with reduced recovery periods….chronic stress occurs from long-term exposure to stressful situations which impeded one's abilities and can result in burnout (Dykstra & Paul, 2018).	1. Acute stress 2. Episodic stress 3. Chronic stress 4. Time stress 5. Anticipation Stress 6. 6. Situational Stress

Source: author synthesis

Stress, workload, awareness, and cognition are some categories that apply to human factors in cybersecurity (Gutzwiller et al., 2019). Given that cybersecurity is a complex socio-technical system, the application of human factors in cybersecurity is continuously emerging as the domain addresses nascent areas (Gutzwiller et al., 2019). Most organizations and business decision-makers lack foundational expertise in managing human factors in cybersecurity—hence, the sustained human performance issues in cybersecurity.

Human performance problems are exacerbated by a shortage of skilled workers, inadequate resourcing, poor management, and ineffective prioritization. Cybersecurity professionals and information technologists work long hours under high demand to prevent cyber attacks, data breaches, and ransomware attacks (Thomas, 2020). A 2019 survey indicated that 91% of Chief Information Security Officers (CISOs) experienced moderate to high-stress levels, and 28% reported that the sustained stress level impeded their performance (Thomas, 2019).

Furthermore, 77% of corporate employees have experienced burnout in their current roles (Thomas, 2020). In a recent survey, 70% of employees emphasized that their businesses perform poorly in averting and reducing burnout (Thomas, 2020). A 2019 survey of 408 CISOs noted that most are dealing with a cybersecurity talent shortage (Nominet Cyber Security, (2019), which adversely contributes to human performance,

often in the form of stress, burnout, and fatigue. The survey pointed out that 17% of CISOs used medication or alcohol to cope with stress, while 60% rarely unplug from their jobs, and 88% reported working more than 40 hours per week (Nominet Cyber Security, (2019). These statistics reflect the pressure and stress at the CISO-level, cascading down the cybersecurity ranks due to the lack of human performance initiatives targeting stress, fatigue, and burnout.

Human performance dilemmas in cybersecurity are exacerbated by many factors, such as remote work, distractions, life-changing events, and a relentless threat environment. For example, a recent survey of 2,000 office workers highlighted that younger employees and employees caring for children or adults reported negative experiences and engaged in riskier online behavior while working remotely (Cunningham, 2021). A contemporary study highlighted that prolonged stress, anxiety, interruptions, and burnout are human performance problems that require proactive leadership engagement (Cunningham, 2021). Compounding issues such as working remotely and constant changes in cybersecurity degrade human performance.

It is known that humans are the most significant vulnerability to your cybersecurity programs (Moustafa, Bello, & Maurushat, 2021); yet, most business decision-makers inadequately address human performance issues. The persistence of human performance problems exists due to an "under-education" on human factors in cybersecurity. Human factors researchers and practitioners need to partner with industry and academia to create human factors educational programs and practical solutions to reduce human performance issues in cyber. For example, federal regulations mandate the working hours per day for airline pilots and flight attendants in the commercial aviation industry. Addressing human performance problems in cybersecurity aims to reduce cybersecurity risks and reinforce positive security behavior.

4.1 Security Fatigue

Security fatigue surfaced in existing literature as early as 2009 when researchers revealed that organizations are prone to inducing security fatigue despite the plethora of technologies and countermeasures to reduce information security risks (Furnell and Thomson, 2009). A 2008 survey of 1,280 respondents indicated that one-third of participants reported that security requirements impeded their jobs (SAI, 2008). Researchers at the National Institute of Standards and Technology raised awareness on security fatigue due to its unimpeded effort and challenges on information security (Stanton et al., 2016). Researchers publish articles on security fatigue (Cram, Proudfoot, & D'Arcy, 2019; Stanton et al., 2016); however, business organizations fail to account for the phenomenon. Nobles (2019) argued that issues such as security fatigue continue to plague information security, cybersecurity, and data privacy because human factors practitioners are not engaged in supporting cybersecurity. Human factors practitioners can evaluate high friction areas and address such issues through improving the system design to reduce problematic areas such as security fatigue.

Researchers defined security fatigue as mental exhaustion after engaging in extended periods of cognitive activity (Serfontein, Drevin, & Kruger, 2018). In addition, Ritchey (2018) classified security fatigue as a weariness or lethargic nature that disregards computer security. Therefore, it is essential to note the various types of fatigue in cybersecurity and the need to annotate and define, as described in Table 1. Table 1 provides a list of documented fatigues in cybersecurity and indicates that the security fatigue phenomenon is complex and progressing. Unfortunately, organizations lack the organic expertise and partnerships to address security fatigue in current-day risk management practices. Therefore, the intricate changes in the cybersecurity domain further acerbate and perpetuate the challenge of remediating fatigue. Bone (2017) underscored that stress, fatigue, and demanding security challenges diminish employees' cognitive abilities, resulting in successful semantic attacks. The increasing number of types of security fatigue requires meticulous initiatives and remediation.

4.2 Types of Security Fatigue

Table 2 Different Types of Security Fatigue

Different Types of Security Fatigue	
Type	**Definition**
Authentication Fatigue	A condition of weariness and tiredness from continuously validating one's identity accompanied by the enforcement of creating complicated passwords, passphrase expirations, and additional credentialing to gain access (Sasse, 2013).
Cognitive Fatigue	A state of mental fog is caused by exhaustion or lethargic behavior stemming from exceeding one's mental acumen with strenuous or high attentional demands and activities for an extended period (Dykstra & Paul, 2019).
Data Breach Fatigue	The concept of consumers becoming complacent to data breaches results in less preparation and less than desirable security practices towards breaches (Kwon & Johnson, 2015; Zorabedian, 2019).
Decision Fatigue	The state of exceeding one's cognitive abilities makes frequent security decisions when manipulating information and computer systems (Ritchey, 2018).
Password Fatigue	An overwhelming experience induced by the practice of committing too many passwords to memory (Napallan, 2018).
Regulatory Fatigue	Tiredness due to overburden of maintaining strict compliance with increasing mandated laws in fear of being non-compliant (Corporate Compliance Insights, 2015).
Operator Fatigue	This type of fatigue occurs as the onset of exhaustion

	and lethargic behavior due to continuous and extensive exposure to cognitively demanding cybersecurity operations (Dykstra & Paul, 2019).
Mental Fatigue	The degradation and depletion of psychological faculties due to monotonous tasks, stress, and periods of inactivity between tasks and functions (Mirilla, Tappert, Frank, & Tao, 2018).
Chronic Fatigue	Formally known as chronic fatigue syndrome, it is a weakening, prolonged-term disorder in which people suffer from exhaustion that is not remediated by rest, a constant state of mental fogginess, and trouble with memory and sleep (Davis, 2018).
Survey Fatigue	The overindulgence of survey testing and various instruments to gather feedback or responses results in lower response rates (Roberts and Allen, 2015).
Alarm Fatigue	This type of mental exhaustion forms many false-positive alerts that distrust alerts (LaManna, 2017).
Threat-Alert Fatigue (Alert Fatigue)	Exhaustion occurs from monitoring and analyzing many incidents to determine the significance of the alerts related to cybersecurity (Aminanto et al., 2019).
Training Fatigue	Ineffective cybersecurity education makes employees frustrated or exhausted, resulting in less responsive training outcomes (MacEwan, 2017).

Source: author synthesis

Safa, Von Solms, and Furnell (2016) indicated a deficiency in security awareness, inexperience, carelessness, apathy, misbehavior, and resistance as salient factors that result in human-enabled errors. The National Institute of Standards and Technology study denoted that security fatigue results in personnel taking increased security risk and practicing non-compliant behavior (Ritchey, 2018). The human element in cybersecurity remains paramount as research and industry trends indicate a continuation of risky security behavior; consequently, leading to business decision-makers placing a heightened emphasis on information security awareness (Serfontein, Drevin, & Kruger, 2018). Researchers postulated that security awareness programs lack the comprehensiveness to address security problems such as security fatigue (Serfontein, Drevin, & Kruger, 2018).

Existing literature on security fatigue could manifest in the management of security and cognitively in executing security-related tasks and functions (Parkins et al., 2016). Researchers suggested that fatigue impacts how an employee consciously and unconsciously attains work objectives (Parkins et al., 2016). In addition, exceeding an employee's cognitive ability during a fatigued state could result in adaptive thinking to determine a solution (Parkins et al., 2016). Although the researchers highlighted some

physiological implications of security fatigue, most fail to connect fatigue to human factors. Other industries such as aviation, medicine, and industrial safety leverage human factor initiatives to address human performance dilemmas (Nobles, 2019).

A growing concern in cybersecurity and information security is the mounting operational demands that result in employee burnout. Cybersecurity fatigue and burnout are growing phenomena exaggerated by a shortage of cyber professionals and an increasingly tumultuous threat landscape (Hinkley, 2019). The relentless demand to protect systems, intellectual property, data, and financial resources increases cybersecurity professionals' anxiety and stress (Hinkley, 2019). A recent Deloitte survey of 1,000 employees indicated that 77% had experienced burnout in their current positions, and more than 50% reported experiencing more than once (Fisher, 2018).

According to Ogbanufe and Spears (2019), cybersecurity professionals are under immense pressure accompanied by a talent shortage that increases operational job stressors, resulting in fatigue and burnout. Security fatigue and burnout require immediate attention from business decision-makers, especially security and technology executives responsible for information security, technology integration, governance, and data privacy. Therefore, it is important to note that security and technology executives struggle to remediate security fatigue and burnout because human factor practitioners are primarily absent in cybersecurity operations (Nobles, 2019).

Security practices and user behavior are often opposing forces due to security fatigue-inducing requirements; consequently, resulting in good security practitioners circumventing security controls (Koppel, Blythe, Kothari, & Smith, 2016). Researchers highlighted that security fatigue is analogous to decision fatigue in that it mandates employees to make choices on depleted mental faculties (Stanton, Theofanos, Prettyman, & Furman, 2016). One study the following effects from decision fatigue, which has a direct correlation to security fatigue (Stanton et al., 2016):

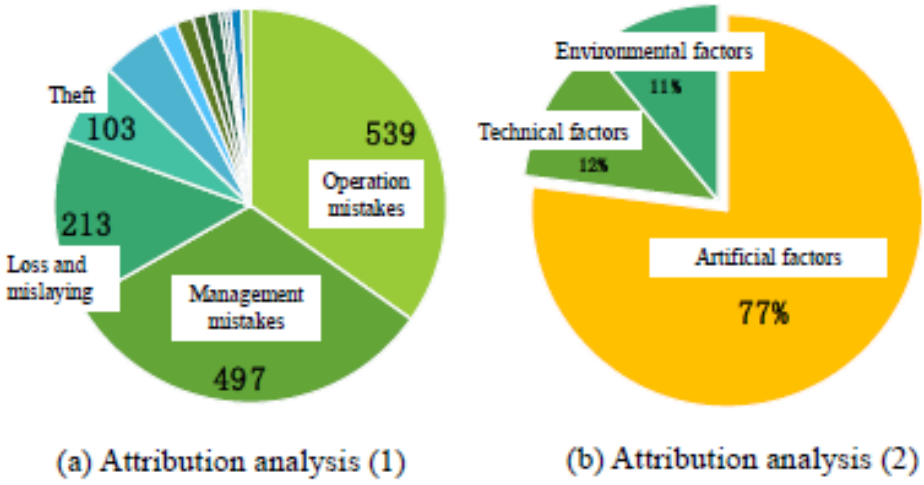
1.) Evading pointless decisions
2.) Selecting the most straightforward option available
3.) Basing decisions on instantaneous motivation
4.) Selecting a simplified algorithm rather than a complicated alternative
5.) Acting impulsively
6.) Feeling overwhelmed and a loss of control

Security fatigue leads to frustration and a less than desirable attitude and behavior to support informational assurance and security policies (Bojanova, Voas, Chang, & Wilbanks, 2016). This further corroborated a study that compared cybersecurity professionals and general users, in which both groups indicated a high level of frustration and powerlessness regarding the information security rules (Koppel et al., 2016). A significant takeaway from the study was that cybersecurity professionals could use the findings of the general users' group to help shape and scope access and password policies that are user-friendly and less frustrating (Koppel et al., 2016). The disconnect between cybersecurity professionals and general users emphasizes the need

for psychology-based professionals to develop less fatigue-inducing policies and practices.

The continuous influx of defensive countermeasures is called out as a stressor that results in security fatigue and burnout syndrome (Tanimoto et al., 2017). For example, research conducted by Tanimoto et al. (2017) in Figure 1, attribution analysis (a) highlights frequent human-induced errors that are categorized in three categories (technical, environmental, and artificial), in which artificial factors illustrates unintended outcomes, such as unintentional human mistakes or errors.

Figure 1 Attribution Analysis of Information Security Incidents



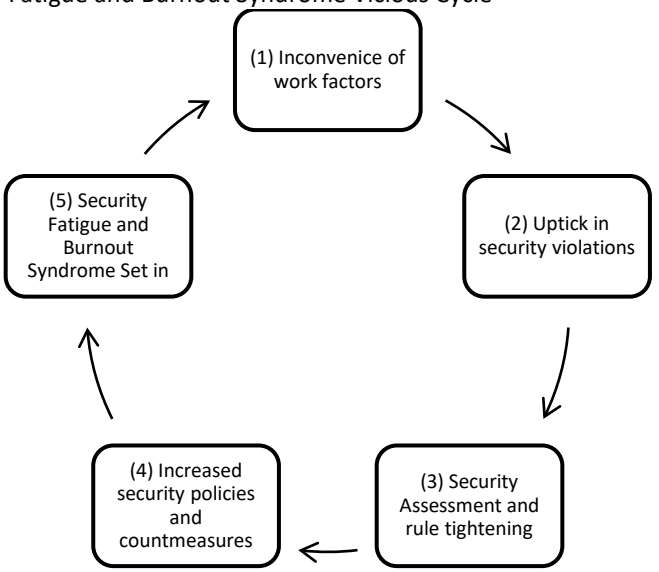
Source Tanimoto et al., 2017

Strict security countermeasures or policies could inadvertently incite unintentional mistakes, as illustrated below to what researchers call a vicious cycle resulting in tightening security policies and rules, accompanied by human-induced errors (Tanimoto et al., 2017). Figure 2 demonstrates the vicious cycle, including security fatigue and burnout syndrome. The steps in Figure 2 are iterative and based on the contrast application of security solutions that increases security fatigue and burnout.

Step 1 of Figure 2 represents the exhaustion of dealing with the constant security modifications and countermeasures that employees view as inconvenient due to the revolving changes (Tanimoto et al., 2017). Step 2 indicates the employees being non-compliant due to the inconveniences driven by the relentless cycle of security changes (Tanimoto et al., 2017). Step 3 serves as a quality assurance check on security compliance (Tanimoto et al., 2017). Step 4 highlights BDM implementing new security controls and policies due to non-compliant behavior (Tanimoto et al., 2017). Step 5

indicates employees suffering from security fatigue and burnout syndrome (see Figure 3) (Tanimoto et al., 2017). Organizational leaders often misdiagnose fatigue, burnout, and stress; consequently, resulting in the continual integration of additional countermeasures. Tanimoto et al. (2017) refer to the unending process of integrating security controls, policies, and countermeasures as the vicious cycle. This method is self-induced and reflects the undervaluing of human factor engineering in cybersecurity.

Figure 2 Security Fatigue and Burnout Syndrome Vicious Cycle



Source Tanimoto et al., 2017

4.3 Burnout

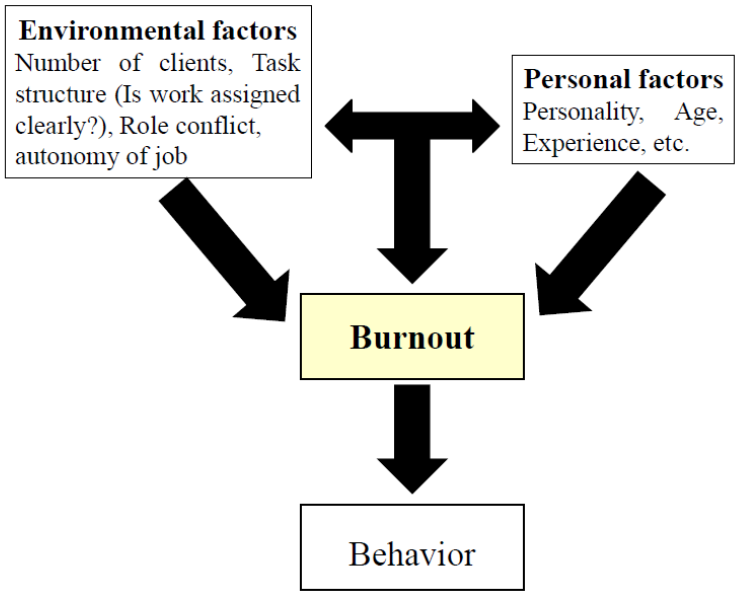
Researchers indicated that burnout is not an individual-based issue but is caused by the workplace climate and environment (Maslach & Leiter, 2005). Maslach and Leiter (2005) emphasized that when organizations neglect to account for the human side of work, a disparity occurs between the nature of work and the disposition of people. According to Signh (2021), the concept of burnout has not been studied in its application to cybersecurity. At issue is the increasing number of cybersecurity attacks and incidents predominantly resulting from human error. A significant gap in cybersecurity is the oversight of human performance and the impact of cybersecurity attacks and incidents.

Valcour (2016) asserted that burnout is derived from a debilitated cognitive state that negatively affects employees' mental and physical health, as previously corroborated in a 2013 study, which inferred that 65% of 5,100 workers in North America suffer operational stressors, loss of control, and extreme fatigue. Researchers have linked burnout to the following health ailments: (a) heart disease, (b) high blood pressure, (c) sleep problems, (d) depression, (e) anxiety, and (f) drug and alcohol abuse (Valcour, 2016). Psychologists deemed burnout as a tri-dimensional problem that consists of (a) exhaustion, (b) cynicism, and (c) inefficacy (Valcour, 2016). Pham (2016, 2019) stressed

that the conceptualization of burnout implies that employees lack interests and undervalue security matters because their jobs take a higher precedent than cybersecurity.

Security compliance burnout is classified as psychological exhaustion and pessimism towards designated security responsibilities based on the lack of interest and underestimating security issues and measures (Pham, 2019). Ross et al. (2009) contended that security controls are designed to motivate employees to comply and have a positive security attitude. Tedious and straightforward tasks can increase security compliance burnout coupled with the continuous implementation of security controls and countermeasures, which increases stress resulting in reduced attention spans (Pham, Brennan, & Furnell, 2019). According to researchers, burnout results from demanding security requirements, the shortage of resources, and the persistent pressure that leads to fatigue (Pham, Brennan, & Furnell, 2019). The result of environmental and personal factors, as depicted in Figure 3, indicates the degradation of human performance due to burnout.

Figure 3 Analytic Model of Burnout



Source Tanimoto et al., 2017

Researchers noted that cybersecurity objectives in insolation hardly result in employee burnout (Choi & Jung, 2018); however, when dealing with a hyperactive cybersecurity threat environment (ENISA, 2021), COVID-19 and disaggregated work are sustained stressors and factors that can result in burnout. Business decision-makers need to assess their employees' work from a holistic perspective to determine if the potential workloads and organizational environments are capable of causing burnout.

According to Nobles (2019), human performance issues persist in cybersecurity due to an underappreciation of human factors and the lack of human-centered design

practices. Amid COVID-19, burnout became a ubiquitous health issue; however, burnout adversely affected the workforce before the most recent pandemic crisis (Thorbecke, 2021), and organizational leaders ignored its debilitation impact on employees. Malasch, a seminal researcher on burnout, refuted the argument that burnout is caused by employees failing to maintain their health (Thorbecke, 2021). The leading cause of burnout is an unhealthy working environment or workplace situation (Thorbecke, 2021). The prominent factor of burnout is exhaustion; researchers emphasized that extreme physical, cognitive, and emotional fatigue are the fundamental catalyst that undercut employees' capacity to work productively and maintain a positive perspective (Maslach & Schaufeli, 2001; Valcour 2016). Inefficacy refers to ineptitude and lack of accomplishments and productivity, while cynicism correlates to attrition of engagement (Valcour, 2016).

4.4 Stress

Organizations continue to fall short on preventing employees' exposure to prolonged stress (Fisher, 2018). The plaguing of stress accounts for more than 120,000 deaths and the healthcare cost of $190B in the U.S. (Moss, 2019). The debilitating impacts of workplace stress result in $500B annually and 550 million days of work lost (Moss, 2019). For example, in a recent industry survey, 70% of the respondents noted that organizations struggle to minimize burnout, while 21% of the survey participants emphasized that their employers do not offer stress-reduction programs. (Fisher, 2018). Reviewing stress in cybersecurity can be explained using the person-environment fit theory. The person-environment fit theory indicates that an imbalance between people and their associated environments increases stress (Edwards, Caplan, & Van Harrison, 1998). Organizational leaders need to ensure an adequate balance between the workplace environment and the employee.

Pham (2019) noted that information security stress had gained the attention of behavioral experts. Existing literature reveals that workplace stress contributes to lower production and non-compliant behavior towards organizational policies and procedures (Pham, 2019). However, some researchers argue that strain, a prolonged stress response, burnout, or work exhaustion improved workers' effectiveness, efficiency, decision quality, and decision accuracy (Monica & Gloria, 2019; Tobler et al., 2017; Wang et al., 2017). Given the evolving nature and constant change in cybersecurity, the person-environment fit is challenged and requires balancing to reduce the onset of stress.

Cybersecurity professionals and information technologists work long hours under high demand to prevent cyber attacks, data breaches, and ransomware attacks (Thomas, 2020). A 2019 survey indicated that 91% of Chief Information Security Officers (CISOs) experienced moderate to high-stress levels, and 28% reported that the sustained stress level impeded their performance (Thomas, 2019). The survey indicated that 17% of CISOs used medication or alcohol to cope with stress, while 60% rarely unplug from their jobs, and 88% reported working more than 40 hours per week (Nominet Cyber Security,

2019). These statistics reflect the pressure and stress at the CISO-level, cascading down the cybersecurity ranks due to the lack of human performance initiatives targeting stress, fatigue, and burnout.

A recent study highlighted that stress had been theorized primarily as a negative phenomenon, as apparent by adverse psychological reactions such as dissatisfaction, fatigue, distress, job turnover, and non-compliant behavior (Singh, 2021). It is essential to note the positive aspects of stress, existing literature highlights that security-related stress increases compliance (Signh, 2021).

Research regarding stress in information security and cybersecurity is expanding. A study conducted by Helkala et al. (2016) revealed cybersecurity professionals experience more severe sleep, nutrition deprivation, and increased physical and physiological stress compared to other employees. Singh (2021) raises an interesting point in that existing research primarily focused on stress derived from information security mandates, while the impact of security-related stress relating to cybersecurity professionals remains unexplored.

5. Lack of Inclusion of Psychology-based Professionals

A failed realization in cybersecurity is the integration of psychology-based professionals (Nobles, 2019). Business decision-makers need to transition solely from technology-focus to psychology-focus, given that security systems are incapable of preventing social engineering attacks (Widerhold, 2014). Human behavior is the crux of cybersecurity, just as technology (Michel, 2017). The research divergence between human performance and behavior in cybersecurity requires the urgent consideration of human factors practitioners and psychology-based experts (Mancuso et al., 2014; Nobles, 2018). Widerhold (2014) emphasized the following areas for leveraging the expertise of psychologists:

1. Understanding end-user behavior and actions towards depicting risks and rewards
2. Identifying and comprehending malicious actors deviant behaviors and designing technological resources to prevent psychological distortion
3. Serving as advisors to politicians for legislation purposes regarding cybercrime
4. Informing the public on the different psychological interplay used by cybercriminals through collaboration with labs, the media, and social networks
5. Understanding the victimization of cybercrime.

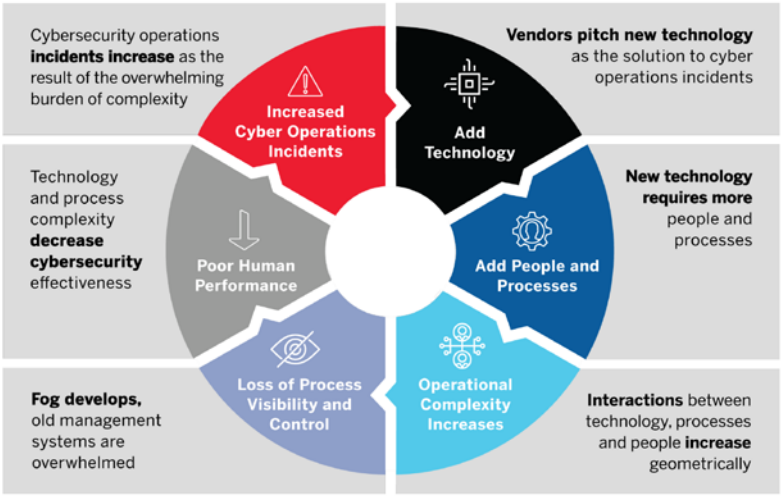
An ongoing trend in cybersecurity is cybercriminals targeting end-users' biases and cognitive vulnerabilities (Michel, 2017). Therefore, including psychology-based professionals in cybersecurity to develop core competencies to mitigate cybersecurity risks by leveraging psychology practices to solidify end-users' approach to compliance and positive security behavior. Cybercriminals capitalize on the psychological gaps in cybersecurity because organizations have extensively integrated technological solutions

while leaving the human element vulnerable (Michel, 2017; Nobles, 2019; Widenhorf, 2014). The failure to include psychology-based professionals in cybersecurity operations prolongs the development of practical solutions to mitigate human behavior in cybersecurity.

6. Breaking the Technology Led Cycle

Technology is the consistent reaction to advancing or responding to a cybersecurity vulnerability, as evident by industries investing $133B in technologies in 2022 (Wilson, Hamilton, & Stallbaum, 2020). Degradations in human performance contribute to most cybersecurity incidents and are the most overlooked aspect in organizations (Wilson, Hamilton, & Stallbaum, 2020). Neglecting to address human performance in cybersecurity perpetuates a continuous cycle of integrating more technologies, increasing the number of people and processes, resulting in complexity debt (Wilson, Hamilton, & Stallbaum, 2020). Below is a depiction of a technology-led cycle that perpetuates cybersecurity incidents (Wilson, Hamilton, & Stallbaum, 2020).

Figure 4 A Technology-led Cycle Leads to Increased Cybersecurity Incidents



Source Wilson, Hamilton, & Stallbaum, 2020

Hardening human performance in cybersecurity is not an easy feat and requires driving new behaviors and understanding through the culture by leveraging human performance as a vital layer of defense (Wilson, Hamilton, & Stallbaum, 2020). Establishing such a layer of security and protection is manifested through a high-reliability organization (HRO), defined as an organization with an unusually low number of incidents consistently over a sustained period (Wilson, Hamilton, & Stallbaum, 2020). A recent study noted that cyber-attacks could lead to stress, anxiety, depression, ailments similar to post-traumatic stress disorder, and internet paranoia (Louie, 2020). Without a doubt, the long-term implications of internet paranoia negatively impact

one's cognitive abilities and increase stress. The practice of HRO is deeply rooted in highly complex technical fields (Wilson, Hamilton, & Stallbaum, 2020), and with cybersecurity being a sociotechnical system and domain, underpinning cybersecurity with HRO initiatives could reduce security incidents.

According to Wilson, Hamilton, and Stallbaum (2020), HRO is fundamentally based on the following three practices: (a) mindfulness, (b) responsiveness, and (c) learning capacity. Researchers expanded the HRO principles to address the human performance gap in cybersecurity through an analogous concept known as high-reliability cybersecurity organizations (HRCO) (Wilson, Hamilton, & Stallbaum, 2020). The pillars for HRCO are depicted in Table 3.

Table 3 High-reliability Cybersecurity Organization Pillars

HRO PILLAR	DESCRIPTION	EXAMPLE APPLICATION IN HRCOS
Formality	• People follow authorized procedures (not workarounds). • They communicate in a disciplined manner to ensure information is consistent and reliable.	• Processes are in place to manage privileged identities, accounts, and information. • Rules are clear for why privilege is conferred, who is responsible, and how it is reviewed.
Level of Knowledge	• People understand not only what they do but why they do it. • They continually expand their understanding of systems, processes, and hazards around them.	• Users understand how easily passwords can be compromised and the risk of unauthorized access. • Everyone uses unique strong passwords and password vaults and supports periodic password changes.
Integrity	• People can be relied upon to do what they say they will and what is expected of them. • They hold themselves and others accountable.	• Employees willingly operate within security policies and use tools as designed/intended. • They do so even if it changes how they do their work (using company-provided devices, limiting downloads or access, regular backups, etc.).
Questioning Attitude	• People anticipate problems and are alert to unusual conditions. • They ask: What could go wrong? What has changed? What might I or others be missing?	• Given the limitations of antivirus filters, employees have a chronic unease about the validity of emails. • Employees check URLs prior to clicking on links and are suspicious of requests for personally identifiable information.
Active Team Backup	• People actively look out for one another. • They understand they are part of something larger than themselves and must work in concert to be effective.	• When configuring new firewall access, team members cross-check/test the updates. • They do so in a planned and structured manner — not out of mistrust but to provide a check to ensure completeness and accuracy.

Source Wilson, Hamilton, & Stallbaum, 2020

The HRCO concept centers on employees attaining a high level of knowledge regarding security, supporting cybersecurity warnings, and demonstrating compliant behavior (Wilson, Hamilton, & Stallbaum, 2020). The pillars of questioning attitude and active team backup ensure reliability by workers adopting a mindset of anticipating problems and supporting each other throughout cybersecurity operations (Wilson, Hamilton, & Stallbaum, 2020). A critical element of HRCO is leading the change through organizational culture to establish resiliency and fewer cybersecurity incidents. Wilson, Hamilton, and Stallbaum (2020) stated the following, "When technology and process

fail, human performance is all that stands between you and a cyberattack". When the inevitable happens, are your employees suffer from security fatigue, stress, or burnout?

7. Recommendations

Currently, there is a human factors knowledge gap in cybersecurity; as a result, human factors practitioners are not deemed critical stakeholders in cybersecurity. This critical omission prevents organizations from leveraging the expertise of human factors. As a result, business organizations struggle with persistent threats and expanding vulnerabilities in cybersecurity while human performance issues continue to mount. The human element remains one of the most underexplored areas in cybersecurity, especially human behavior and human performance. Stress, security fatigue, and burnout negatively impact employees' ability to maximize cybersecurity. As illustrated in Figure 4, technology-led dependency creates technical and complexity debt that degrades human performance and results in a continuous cycle of cybersecurity incidents (Wilson, Hamilton, & Stallbaum, 2020). Below are recommendations to integrate human factors engineering to enhance human performance in cybersecurity.

Partner with Human Factors Experts. Organizations should partner with human factors practitioners to address the high friction areas that impede human performance in cybersecurity. Human factors practitioners can provide expertise in understanding the technological implications and the adverse influence on employees from the fast pace of technology (Hollnagel, 2016), especially the growth in cybersecurity. The increasing demand for faster, better, and cheaper to attain higher levels of productivity and performance through technological innovation is an essential human factor challenge (Hollnagel. 2016). Unfortunately, organizations failed to account for the human element by excluding human factors practitioners from contributing to these scientific evolutions—which most organizations take for granted. The expertise of human factors practitioners can help eliminate the unintended consequences stemming from not accounting for humans and change the ways of work through technical means. Cybersecurity is a sociotechnical system that requires a high level of availability, functionality, and automation. Few organizations account for the human element when designing systems in cybersecurity—hence a human factors practitioner can provide the necessary expertise.

Implement a Human Factors Program. In addition to partnering with human factors practitioners, it is prudent to implement a Cybersecurity Human Factors Program for organizations with large and complex cybersecurity programs. A human factors program in cybersecurity could improve the salient factors such as cybersecurity awareness and security training to prevent security fatigue, not only to cybersecurity and information security professionals but also non-technical personnel (Nobles, 2019). Implementing a human factors program aims to reduce the high friction areas that result in cybersecurity incidents such as degraded human performance. Such programs have

proven effective in aviation, medicine, nuclear power, and industrial safety (Nobles, 2019) and should emphasize cybersecurity.

Practice Human-Centered Cybersecurity. As cybersecurity continues to evolve, the complexity increases; thus, making it difficult for people to manage and comprehend the systems within the system. A human-centered (design thinking) cybersecurity approach is vital to ensure people are a centric pillar when developing systems. Human-centered design is a common practice in human-computer interaction that incorporates human factors when engineering human interfaces in computing (Boy, 2017). Complex systems such as cybersecurity require rigorous focus on people and organizations when designing systems to ensure human performance is not degraded or impeded when interacting with the technologies (Boy, 2017), security policy compliance, change management, and regulatory guidance. Evaluating cybersecurity task analysis through a human-centered lens could provide a deeper understanding of tasks such as differentiating critical tasks from routine tasks.

Establish Anti-Fatiguing Programs. The degradation of human performance in cybersecurity is a critical problem deserving the immediate attention of business decision-makers. Even though I only discussed stress, burnout, and security fatigue, there is an extensive list of human performance challenges in cybersecurity that are unmitigated and explored by cybercriminals. Other sociotechnical industries have tackled human performance problems, and now is the time for the cybersecurity industry to get serious about human factors. Implementing an anti-fatiguing initiative is one way to address human performance degradation, especially exploring factors causing stress, burnout, and fatigue and subsequently integrating prevention measures. Stress, burnout, and security fatigue existed long before COVID-19. The pandemic highlighted these human performance issues and how cybercriminals exploit people to execute cyber-attacks. Human performance issues remain unmitigated and open vectors for subsequent attacks without an anti-fatiguing program.

8. Conclusion

Human performance issues such as stress, burnout, and security fatigue are critical concerns in cybersecurity. However, organizations are lethargic to address these issues other than through technological means. As pointed out, technology-led cycles are problematic and increase complexity debt that results in degraded human performance. The constant technology changes coupled with a hyperactive cybersecurity threat environment takes a toll on all employees. Cybercriminals target human weaknesses as a vector to attack organizations because most businesses fail to solidify the human element—technology alone is not enough. Organizations can reinforce cybersecurity practices by learning from other industries and implementing human factors initiatives to prevent human performance degradation. Stress, burnout, and security fatigue are human risk factors that require mitigation and eradication to reduce the organization's chances of experiencing a successful cyber-attack or incident.

References

Aminanto M.E., Zhu L., Ban T., Isawa R., Takahashi T., Inoue D. (2019) Combating threat-alert fatigue with online anomaly detection using isolation forest. In: Gedeon T., Wong K., Lee M. (eds) Neural Information Processing. ICONIP 2019. Lecture Notes in Computer Science, vol 11953. Springer, Cha

Bojanova, I., Voas, J., Chang, M., & Wilbanks, L. (2016). Cybersecurity or Privacy [Guest editors' introduction]. *I.T. Professional*, *18*(5), 16-17.

Bone, J. (2017). *Cognitive Hack: The New Battleground in Cybersecurity... the Human Mind*. CRC Press.

Boy, G. A. (2017). Human-centered design of complex systems: An experience-based approach. *Design Science*, *3*.

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

Cong Pham, H., Brennan, L., & Furnell, S. M. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications.* Retrieved from http://hdl.handle.net/10026.1/13591. DOI: 10.1016/j.jisa.2019.03.012

Corporate Compliance Insights. (2015, May 13). Retrieved from https://www.corporatecomplianceinsights.com/thomson-reuters-annual-cost-of-compliance-survey-shows-regulatory-fatigue-resource-challenges-and-personal-liability-to-increase-throughout-2015/

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2019). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*.

Cunningham, M. (2021, March 25). "Tiny crimes" – How minor mistakes when remote working could lead to major cybersecurity breaches (Part 1). Forcepoint.com. Retrieved from https://www.forcepoint.com/blog/x-labs/minor-mistakes-major-breaches-pt-1.

Cybenko, G., Giani, A., & Thompson, P. (2002). Cognitive hacking: A battle for the mind. *Computer*, *35*(8), 50-56.

Davis, N. (2018, December 17). Chronic fatigue syndrome could be triggered by overactive immune system. TheGuardian.com. Retrieved from https://www.theguardian.com/society/2018/dec/17/chronic-fatigue-syndrome-could-be-triggered-by-overactive-immune-system

Dykstra, J., & Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. In *11th USENIX Workshop on Cyber Security Experimentation and Test CSE, 18*.

Edwards, J. R., Caplan, R. D., & Van Harrison, R. (1998). Person-environment fit theory. *Theories of organizational stress*, *28*(1), 67-94.

ENISA Threat Landscape 2021. (2021, October). Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Fisher, J. (2018, July 31). How managers can prevent their teams from burning out. Retrieved from https://hbr-org.cdn.ampproject.org/c/s/hbr.org/amp/2018/07/how-managers-can-prevent-their-teams-from-burning-out

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

Grier, R. A. (2015, September). How high is high? A meta-analysis of NASA-TLX global workload scores. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 59, No. 1, pp. 1727-1731). Sage CA: Los Angeles, CA: SAGE Publications.

Gutzwiller, R. S., Cosley, D., Ferguson-Walter, K., Fraze, D., & Rahmer, R. (2019, November). Panel: Research sponsors for cybersecurity research and the human factor. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 63, No. 1, pp. 422-426). Sage CA: Los Angeles, CA: SAGE Publications.

Helkala, K., Knox, B., Jøsok, Ø., & Knox, S. (2016). Factors to affect improvement in cyber officer performance. *Information & Computer Security*.

Hinkley, C. (2019 September 16). Preventing PTSD and burnout for cybersecurity professionals. Darkreading.com. Retrieved from https://www.darkreading.com/risk/preventing-ptsd-and-burnout-for-cybersecurity-professionals/a/d-id/1335750?fbclid=IwAR31h9dqAsT7oC5JaAEGseXlSnL1C1Jp5VsntlFGwDaFy4Pf82JSCIbFTUU

Hollnagel, E. (2016). The nitty-gritty of human factors. *Human factors and ergonomics in practice: Improving system performance and human well-being in the real world*, 45-64.

Hull, J. L. (2017). *Analyst Burnout in the Cyber Security Operation Center-CSOC: A Phenomenological Study* (Doctoral dissertation, Colorado Technical University).

ISACA. (2020, November 18). Understanding and burning CISO burnout. ISACA.org. Retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2020/understanding-and-addressing-ciso-burnout

Koppel, R., Blythe, J., Kothari, V., & Smith, S. (2016). Beliefs about cybersecurity rules and passwords: A comparison of two survey samples of cybersecurity professionals versus regular users. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*.

Kwon, J., & Johnson, M. E. (2015, June). The market effect of healthcare security: Do patients care about data breaches?. In *WEIS*.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

LaManna. M. (2017). Technology intercepts for cyber security applied to critical infrastructures. *WMSCI* ,8-11.

Loui, R. K. (2020, February 28). #Psybersecurity: Mental healths impacts of cybersecurity attacks. RSA Conference 2020. San Francisco, California

MacEwan, N. (2017). *Responsibilisation, rules and rule-following concerning Cyber Security: Findings from Small Business Case Studies in the U.K.* (Doctoral dissertation, University of Southampton).

Maslach, C., and Schaufeli, W. (2001). Job burnout. *Annual Review of Psychology* (52), pp. 397–422.

Maslach, C., & Leiter, M. P. (2005). Reversing burnout. *Standford Social Innovation Review*, 43-49.

Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014, September). Human factors of cyber-attacks: a framework for human-centered research. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, pp. 437-441). Sage CA: Los Angeles, CA: SAGE Publications.

Michel, A. (2017). Psyber Security: Thwarting Hackers with Behavioral Science. *APS Observer*, *30*(9).

Mirilla, D. F., Tappert, C. C., Frank, R. I., & Tao, L. (2018). A proposed dynamic Security Operations Center Management Framework for reducing task disengagement. *Proceedings of Student-Faculty Research Day*, Pace University.

Monica, A., & Gloria, P. W. (2019). Stressed decision-makers and use of decision aids: a literature review and conceptual model. *Information Technology & People*, *33*(2), 710- 754. https://doi.org/10.1108/ITP-04-2019-0194

Moss, J. (2019, December 11). Burnout is about your workplace, not your people. HBR.org. Retrieved from https://hbr-org.cdn.ampproject.org/c/s/hbr.org/amp/2019/12/burnout-is-about-your-workplace-not-your-people

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving *cyber security management.* Frontiers in Psychology*,* 12.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.

Nobles, C. (2019). Establishing human factors programs to mitigate blind spots in cybersecurity. *MWAIS 2019 Proceedings*, 22. https://aisel.aisnet.org/mwais2019/22

Nobles, C. (2021a, February 8). The Human Factors Series: Burnout and fatigue are sustained problems in cybersecurity. https://www.linkedin.com/pulse/human-factors-series-burnout-fatigue-sustained-calvin-nobles-ph-d-/ [post]. LinkedIn. https://www.linkedin.com/pulse/human-factors-series-burnout-fatigue-sustained-calvin-nobles-ph-d-/

Nominet Cyber Security. (2019). Life inside the perimeter: Understanding the modern CISO. Retrieved from Nominet-Cyber_CISO-report_FINAL-130219.pdf.

Nori, P., Bartash, R., Cowman, K., Dackis, M., & Pirofski, L. A. (2019, April). Is burnout infectious? Understanding drivers of burnout and job satisfaction among academic infectious diseases physicians. In *Open forum infectious diseases* (Vol. 6, No. 4, p. ofz092). U.S.: Oxford University Press.

Ogbanufe, O., & Spears, J. (2019). Burnout in cybersecurity professionals. Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy, Munich, Germany, December 15, 2019.

Okereafor, K., & Adelaiye, O. (2020). Randomized cyber attack simulation model: a cybersecurity mitigation proposal for post covid-19 digital era. *International Journal of Recent Engineering Research and Development (IJRERD)*, *5*(07), 61-72.

Parkin, S., Krol, K., Becker, I., & Sasse, M. A. (2016). Applying cognitive control modes to identify security fatigue hotspots. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489-510.

Pham, H.-C., El-Den, J., & Richardson, J. (2016). Stress-based security compliance model – an exploratory study. *Information and Computer Security*, *24*(4), 326.

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

Platsis, G. (2019). The Human Factor: Cyber Security's Greatest Challenge. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1-19). IGI Global.

Platsis, G. (2019, August 14). Is staff burnout the best reason to implement cybersecurity A.I.? Securityintelligence.com. Retrieved from https://securityintelligence.com/articles/is-staff-burnout-the-best-reason-to-implement-cybersecurity-ai/

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*, *11*(1), 21582440211000049.

Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches? *Security & Privacy, IEEE* 10 (3), 57-63.

Roberts, L. D., & Allen, P. J. (2015). Exploring ethical issues associated with using online surveys in educational research. *Educational Research and Evaluation*, *21*(2), 95-108.

Ritchey, D. (2018). Curing security fatigue. *Security, 55*(9), 10. Retrieved from http://libproxy.temple.edu/login?url=https://search-proquest-com.libproxy.temple.edu/docview/2109287230?accountid=14270

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security*, *56*, 70-82.

SAI Global. (2008). SAI Global Information Security Awareness Survey 2008. Retrieved from http://www.saiglobal.com

Sasse, M. A. (2013, August). Technology should be smarter than this!: A Vision for Overcoming the Great Authentication Fatigue. In *Workshop on Secure Data Management* (pp. 33-36). Springer, Cham.

Serfontein, R., Drevin, L., & Kruger, H. (2018). The feasibility of raising information security awareness in an academic environment using SNA. In *IFIP World Conference on Information Security Education* (pp. 69-80). Springer, Cham.

Singh, T. (2021). *The role of stress among cybersecurity professionals* (Doctoral dissertation, The University of Alabama).

Sheridan, K. (2020, June 6). 90% of CISOs would pay for better work-life balance. DarkReading.com. Retrieved from https://www.darkreading.com/risk/90--of-cisos-would-cut-pay-for-better-work-life-balance/d/d-id/1336995

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *I.T. Professional*, *18*(5), 26-32.

Tanimoto, S., Nagai, K., Hata, K., Hatashima, T., Sakamoto, Y., & Kanai, A. (2017, July). A Concept Proposal on Modeling of Security Fatigue Level. In *2017 5th Intl Conf on Applied Computing and Information Technology/4th Intl Conf on Computational Science/Intelligence and Applied Informatics/2nd Intl Conf on Big Data, Cloud*

Thomas, B. (2019, December 26). Most urgent CISO skills 2020: Reporting avoiding burnout, more. Bitsight.com. Retrieved from https://www.bitsight.com/blog/5-shocking-it-cybersecurity-burnout-statistics.

Thomas, B. (2020, January 07). Five shocking I.T. and cybersecurity burnout statistics. Bitsight.com. Retrieved from https://www.bitsight.com/blog/5-shocking-it-cybersecurity-burnout-statistics.

Thorbecke, C. (2021, July 02). Why business leaders need a wake-up call to take burnout seriously right now, experts say. Yahoo.com. Retrieved from https://www.yahoo.com/gma/why-business-leaders-wake-call-100007147.html

Tobler, N., Colvin, J., & Rawlins, N. W. (2017). Longitudinal analysis and coping model of user adaptation. *Journal of Computer Information Systems*, *57*(2), 97-105. https://doi.org/10.1080/08874417.2016.1183415

Valcour, M. (2016). Beating burnout. *Harv Bus Rev*, *94*, 98-101.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*,*28*(2),378-396. https://doi.org/10.1287/isre.2016.0680

Wilson, S., Hamilton, & Stallbaum, S. (2020, May 26). The unaddressed gap in cybersecurity: Human performance. *MIT Sloan Management Review*. Retrieved from https://sloanreview.mit.edu/article/the-unaddressed-gap-in-cybersecurity-human-performance/

Zorabedian, J. (2019, February 01). Data breach fatigue makes every day feel like groundhog day. SecurityIntelligence.com. Retrieved from https://securityintelligence.com/data-breach-fatigue-makes-every-day-feel-like-groundhog-day