INSTITUTE FOR HOMELAND SECURITY

Security Fatigue as Insider Threat:

Sources, Consequences, and Mitigation

Peter S. Lehmann, Ph.D.

Contents

Abstract

Scholarly attention increasingly has focused on the importance of “unintentional insider threats” where well-intentioned individuals operating within an organization inadvertently facilitate a cyberattack from an outsider. These unintentional insider threats are sometimes linked to “security fatigue,” which is defined as a gradual decay in sensitivity toward potential security risks. Although personnel may initially follow good security practices, they can drift into a mode of complacency and disillusionment in which they undervalue their own role in risk mitigation or perceive the future threat as either inevitable or highly unlikely. In hospitals and healthcare facilities, the staff responsible for helping to prevent data breaches are especially susceptible to security fatigue due to workload demands. In this report, I discuss the concept of security fatigue, describe its key inputs and contributing factors, and explain how it may be understood in light of the social-psychological literature on information processing, decision-making, and compliance with various rules and policies. Additionally, I review the literature on the consequences of security fatigue in healthcare settings, emphasizing how human factors can undermine the cybersecurity infrastructure designed to protect patient data. Finally, I identify some potential mitigation strategies that hold promise for reducing security fatigue among healthcare personnel.

Keywords: Security fatigue, healthcare, decision-making, cybersecurity, information technology

Introduction

The functioning of the modern healthcare structure in the United States is highly dependent on technology, and the electronic systems used to collect, store, and share confidential patient records are vulnerable to cyberthreats (Martin et al., 2017; Tully et al., 2020). These attacks against hospitals have tripled in the last decade, and more than 42 million patients have had their private data rendered vulnerable by ransomware attacks (Alanzi, 2023; Wasserman & Wasserman, 2022). Patient records are very valuable and thus are frequently targeted by malicious actors (Coventry & Branley, 2018; Neprash et al., 2022; Williams et al., 2020), with healthcare facilities representing the victims of 24% of all cyberattacks (Argaw et al., 2020). One recent report revealed that nearly 90% of healthcare institutions have experienced such an attack (Reeves, 2024)—an estimate that has stayed consistent since 2014 (Perakslis, 2014). Rural hospitals and those using outdated equipment are particularly at risk (Ewoh & Vartiainen, 2024; Neprash et al., 2024; Sullivan et al., 2023), though even large hospital networks located in urban centers can experience data breaches (Cornejo, 2025).

Successful cyberattacks require a point of entry, and mitigation and prevention efforts typically prioritize closing these vulnerabilities by strengthening firewalls and updating hardware and operating systems (Allen, 2024; Ghayoomi et al., 2021). While protecting against external threats via these methods is crucial, scholarly attention increasingly has been directed toward understanding “insider threats” to information security (Choi et al., 2018), as more than 50% of data breaches—and often the most damaging of these events—originate from an actor within the institution (Lee, 2022). Conventional definitions of who or what might be an insider threat primarily call attention to malicious actors motivated to commit deliberate acts of sabotage against an organization, with these events sometimes described as a form of workplace violence (Costa, 2017). However, experts also emphasize the importance of so-called “unintentional insider

threats," where well-intentioned individuals operating within an organization can inadvertently facilitate an attack from an outsider. A report from the CERT Insider Threat Team (2013) defines this concept in the following way:

An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. (p. 2)

Unintentional insider threats to cybersecurity are typically the result of human factors, which are especially relevant in a hospital setting given the heavy cognitive load shouldered by healthcare staff (Burrell, 2024; Nifakos et al., 2021; Willing et al., 2021).

Furnell and Thomson (2009) introduced the concept of "security fatigue" to describe the gradual decay in sensitivity to security threats that occurs when people are required to implement proactive risk-mitigation measures that they do not fully understand or appreciate. Although some individuals "simply disregard security or cannot be bothered with it at all," security fatigue is different in that it occurs when people "have actually been following good practice and then drift (or completely switch) into a mode in which they become tired or disillusioned with it" (p. 7). Furnell and Thomson (2009) also suggest that "there is a threshold at which it simply gets too hard or burdensome for users to maintain security" (p. 7), and once people reach this saturation point they become accustomed to the enduring presence of potential threats such that they are no longer motivated to engage in preventative action (see also Norton et al., 2025; Viseu et al., 2004). Security fatigue can be exacerbated when personnel underestimate the severity of the threat, perceive the issue as low priority, have not fully embraced their own personal role in maintaining security, or view such efforts as someone else's responsibility (Cram et al., 2021; Furnell, 2010, 2021). As Stanton et al. (2016) explain:

We define fatigue as a type of weariness, a reluctance to see or experience any more of something. When these feelings are related to security, we use the term security fatigue. Although other factors might be included in security fatigue, including vigilance and loss of control, this article focuses on the role that decision fatigue plays and the affective manifestations resulting from it. This weariness often manifests as resignation or a loss of control in people's responses to online security. People are told they need to be constantly on alert, constantly "doing something," but they are not even sure what that something is or what might happen if they do or do not do it. (pp. 1-2)

Problem Statement and Research Objective

This report has four primary goals.

- First, I define and discuss the concept of security fatigue.
- Second, I explain how it may be better understood in light of the social-psychological literature on information processing, decision-making, and compliance with regulations, policies, and norms.
- Third, I review the literature on the consequences of security fatigue in healthcare settings, highlighting the types of cyberattacks in which human factors are exploited with the goal of undermining the security infrastructure designed to protect patient data. Finally, I conclude by drawing on prior research that identifies some mitigation strategies that might help reduce security fatigue among healthcare personnel and minimize its harmful effects. By integrating scholarship across multiple fields, this report aims to be an informational resource for policymakers, professionals, and members of the public.

Defining And Understanding “Security Fatigue”

Security fatigue occurs when individuals’ desire to contribute to workplace security is depleted over time, leading them to devalue their own role in security and deprioritize cybersecurity protocols in favor of more pressing tasks (Furnell, 2021; Reeves et al., 2021; Stanton et al., 2016). Although a gradual increase in apathy toward security concerns and protocols is often attributed to IT personnel (Bhana & Ophoff, 2023; Nobles, 2022), the phenomenon extends far beyond this population. Additionally, security fatigue should not be confused with defiant non-compliance among users whose dissatisfaction with working conditions or management manifests as resentment toward organizational security (Hwang et al., 2017; Norton et al., 2025). As Cram et al. (2021) explain:

In a work context, employees who experience security fatigue and engage in non-compliant security behavior for this reason are distinct from those employees who consistently ignore or refuse to comply with security policies. Rather, security-fatigued employees may have at one time been very inclined to comply with security policies, and may still be, but strict compliance is less likely for these employees due to their fatigued state (Furnell & Thomson, 2009). Simply put, these employees are weary of, and worn out by, the demands imposed by security policy requirements, which can have negative consequences for organizational information security efforts. (p. 522)

Although security fatigue is a clear example of a “human factor” that may compromise cybersecurity efforts, to describe it only as a weakness of individual decision-makers is counterproductive. Instead, security fatigue is better understood as a form of decision fatigue that occurs when cognitive resources are depleted (Stanton et al., 2016). In this way, security fatigue represents systematic challenge in an organizational context where demands on users’ mental faculties are already high (Khadka & Ullah, 2025; Nobles, 2022; Reeves et al., 2021). Healthcare providers in particular experience

significant fatigue and burnout, which can lead to the unintentional actions that render hospital information systems vulnerable to cyberthreats (Burrell, 2024; Nifakos et al., 2021; Wasserman & Wasserman, 2022). However, Stanton and colleagues (2016) argue that security fatigue also affects members of the public, informing how average users perceive online security risks and take action to protect themselves. In this way, security fatigue is not restricted to any specific population, as it generally occurs "when individuals are asked to make more decisions than they can process" and thus feel "a sense of resignation and a loss of control" (Stanton et al., 2016, p. 4).

Furnell and Thomson (2009) describe three key inputs to security fatigue: (1) effort, (2) difficulty, and (3) importance. *Effort* relates to the requirements of the security protocol for the user to achieve compliance; some efforts remain fixed and consistent over time, while other activities are increasingly demanding for users (e.g., the task of remembering an ever-growing list of unique passwords). *Difficulty* refers to the ease with which the user can deliver the required effort, thus signifying "how the security concept has been realized in practice" (Furnell, 2021, p. 2289). Finally, *importance* is defined as "how the user perceives and prioritizes the need to secure a given asset," which "reflects their motivation to keep going despite effort and convenience issues of the related controls" (Furnell & Thomson, 2009, p. 9). Notably, the *difficulty* and *importance* of a task can be driven by a variety of individual- and organizational-level influences, including users' understanding of the technology and the extent to which an organizational culture prioritizes security. Moreover, these three inputs are interrelated—the fatigue-inducing effects of *effort* and *difficulty* amplify and reinforce each other, and these forces are reduced when *importance* is higher:

$$\text{Security Fatigue} = \frac{(\text{Effort} \times \text{Difficulty})}{\text{Importance}}$$

Furnell (2021) further describes six specific factors that contribute to security fatigue via their effects on perceived *effort* and *difficulty*. These factors are (1) repeated warnings

about threats that users rarely see; (2) repeated and/or time-consuming actions that are required of users in the name of security; (3) the required use of security controls and processes with an unclear purpose or benefit; (4) being confronted with complicated or unintelligible security technologies; (5) the required use of multiple security methods and mechanisms on different systems and devices that seek to achieve the same goal; and (6) experiencing a high volume of security-related encounters during routine, day-to-day use of devices and services. Building on these ideas, Nobles (2022, pp. 56-57) identifies 13 subtypes of security fatigue that users of information systems might experience, including cognitive fatigue (i.e., "a state of mental fog" that stems from "exceeding one's mental acumen with strenuous or high attentional demands and activities for an extended period"), password fatigue, regulatory fatigue (i.e., originating from "maintaining strict compliance with increasing mandated laws in fear of being non-compliant"), alarm fatigue, and training fatigue.

The Social Psychology of Security Fatigue

To better understand the phenomenon of security fatigue, it can be informative to frame it within the scholarly literature on compliance generally. Encouraging individuals to conform to the requirements of policies, regulations, and other norms is a long-standing problem within organizations (e.g., Cialdini & Goldstein, 2004; Jancsics et al., 2023; Zadeh & Haggerty, 2023), and a variety of potential barriers to compliance have been emphasized in the literature (Makkai & Braithewaite, 1991; Martinez-Moyano et al., 2014). Such barriers may include insufficient or uncertain incentives, ineffective monitoring and enforcement, lack of information or experience, restricted autonomy, cognitive and decision-making limitations, and various attitudinal and belief-related influences (Weaver, 2014). Importantly, while compliance is a crucial part of a functioning bureaucracy and violating norms and regulations can have disastrous consequences, non-compliance is far from rare (see, e.g., Coleman, 1987; Martin et al., 2013; Palmer, 2012). As Jancsics et al. (2023) explain:

Rank-and-file employees as well as managers in public, nonprofit, and private organizations break minor or more serious rules on a daily basis, and often whole organizations are noncompliant with government regulations. Scholars have argued that such rule breaking is not an abnormal condition at all but rather constitutes the essence of everyday bureaucratic routine. (p. 1274)

In some contexts, widespread non-compliance may suggest that a directive is problematic and needs to be revisited, and “constructive non-compliance” (Tsai, 2015) can even be a driver of institutional reform (Feige, 1999; Gofen, 2015; Schnelle, 2025).

The role of fatigue as a source of non-compliance has been studied extensively (Ada et al., 2025; Millington et al., 2022), and cybersecurity-related fatigue in particular has received considerable attention among experts in recent years (Burkitt & Hutabarat, 2023; Cram et al., 2021; Khadka & Ullah, 2025; Norton et al., 2025). Further, research evidence suggests that compliance cannot be improved through training alone. The amount of cybersecurity training that an employee has had is only weakly associated with their competence in handling a real-world cyberthreat (Pattinson et al., 2016), and more frequent training is sometimes associated with reduced risk awareness (Parsons et al., 2013). Because security fatigue is not a technical failure but instead is a social-psychological response to security-related training and concerns, some insights about human cognition, emotion, and decision-making from multiple social science disciplines can be insightful. Importantly, some of the scholarship in this area (e.g., Reeves et al., 2021) introduces several additional concepts and distinguishes between sources of fatigue (i.e., action vs. advice), though providing a comprehensive framework that incorporates these elements is beyond the current scope.

The first key concept is *bounded rationality*, which relates to limitations in the amount of information that humans can process, incomplete or inaccurate information, our own cognitive limitations, and inadequate time to make decisions in light of that information. Bounded rationality is a characteristic of heuristic decision-making (Kahneman, 2003,

2011), which is faster and requires less effort than systematic thinking but is compromised by a lack of accuracy due to a heavy reliance on mental shortcuts and biases (Acquisti & Grossklags, 2007; Luo et al., 2013). In the context of organizational policies and regulations, these ideas are closely linked to Beautement and colleagues' (2008) notion of the *compliance budget*, where individuals weigh the costs and benefits of compliance and then adapt their behavior toward non-compliance when the barriers associated with compliance are too high relative to the lack of perceived benefits (see also Adams & Sasse, 1999; Stanton et al., 2016). Bhana and Ophoff (2023) connect these ideas to *risk homeostasis*, whereby individuals "compare their perceived risk against their target level risk and adjust their behavior to bridge any incongruity between the two, thus, achieving homeostatic equilibrium" (p. 268).

These existing limitations to rational decision-making can be aggravated by fatigue. According to the "strength model" in social psychology (see, e.g., Baumeister & Vohs, 2007; Duckworth et al., 2018; Hagger et al., 2010; Muraven & Baumeister, 2000), *ego depletion* occurs following the expenditure of cognitive resources, thereby diminishing performance on future tasks due to a lack of motivation or capacity. Cybersecurity diligence requires effortful self-regulation, and the ability to use systemic thinking rather than heuristic thinking when assessing a potential threat can be compromised among individuals whose self-control resources have been drained. Moreover, ego depletion and non-compliance are more commonplace in professional environments where employees are overworked and burned out, as these contexts can produce feelings of exhaustion with and cynicism toward security protocols (Demerouti et al., 2001, 2010; Reeves et al., 2021; Trépanier et al., 2015). The effects of workplace-related factors can be further amplified by *technostress* (D'Arcy et al., 2014; Tarafdar et al., 2010), which arises when individuals perceive that technology is increasing rather than reducing their workload, is too complex to understand, and is evolving too rapidly for them to catch up (Alobayli et al., 2023; Califf et al., 2020; Stadin et al., 2020).

Taken together, the literature on the cognitive and attitudinal origins of security fatigue presents a more complex picture of human decision-making than Furnell and Thomson's (2009) definition might imply. Specifically, security fatigue extends beyond growing disillusionment and apathy toward security concerns over time but is also linked to cognitive resources, as "even if their attitude to cyber security is favorable, employees may begin to make mistakes due to depletion resulting from the often-repetitive behaviors required to maintain cyber security" (Reeves et al., 2021, p. 11). Accordingly, additional training may temporarily increase awareness of security risks among personnel, but these efforts ultimately can prove to be counterproductive because they contribute to already-overburdened mental workloads (Cram et al., 2021; Hore et al., 2024; Nobles, 2022). Further, while decision-making is often constrained by insufficient time and limited information, security fatigue and its consequences arguably are rational from the perspective of the actors involved (Bhana & Ophoff, 2023; D'Arcy et al., 2014; Herley, 2009). Indeed, in response to the overload, complexity, and uncertainty associated with ever-evolving cybersecurity efforts, individuals may view further personal actions as beyond what their compliance budget allows:

While users' cybersecurity behavior is often portrayed as irrational, in fact it might be quite rational and reflect an astute cost-benefit analysis that results in users choosing to ignore "complex security advice that promises little and delivers less." We argue that users experience a sense of security fatigue that also contributes to this cost-benefit analysis and reinforces their ideas about the lack of benefit for following security advice. From this perspective, we in the IT community need to rethink the way we currently conceptualize the public's relationship to cybersecurity. Current mental models that position cybersecurity as something that is not worth the effort will be challenging if not impossible to change. Yet, as IT professionals, it is our responsibility to take up this challenge and work to alleviate the security fatigue users experience. (Stanton et al., 2016, p. 8)

Security Fatigue in Healthcare Settings

As “the proliferation of digitalization increases the surface attack areas of private and public organizations” (Nobles, 2022, p. 51), there has emerged a growing need for effective cybersecurity measures that protect software-based healthcare technology (Coventry & Branley, 2018). Considerable attention has been directed to mitigating the harms posed by malicious external actors, particularly as the interconnected systems and devices that share sensitive information and monitor patients can be vulnerable to attack (Anwar et al., 2021; Ayala, 2016; Ewoh & Vartiainen, 2024; Langer, 2017). Nearly all hospitals have relied upon electronic health records (EHRs) for at least the past decade (Parasrampuria & Henry, 2019), and millions of “Internet of Medical Things” (IoMT) devices collect, analyze, and transmit patient data to inform treatment decisions (Ghubaish et al., 2020; Hatzivasilis et al., 2019; Papaioannou et al., 2022; Thomasian & Adashi, 2021). Medical equipment and information-sharing systems are frequent targets of cyberattacks (Ghayoomi et al., 2021), and healthcare facilities are highly motivated to protect themselves against these events given their frequency and significant costs (Argaw et al., 2020; Portela et al., 2023; Sunil & Mathew, 2024).

The technical aspects of information security are central for defending against some of the external cyberattacks that hospitals commonly encounter, including cryptographic attacks, SQL injections, privilege escalation, and Man-in-the-Middle (MitM) attacks (Bhuyan et al., 2020; Dameff et al., 2023; Wasserman & Wasserman, 2022). Notwithstanding the role of a robust IT infrastructure, “insider threats” that occur via the exploitation of human vulnerability are just as salient a concern as bad actors operating from outside an organization (Coventry & Branley, 2018; Lavanya et al., 2024; Nifakos et al., 2021). As Lee (2022) explains, “one of the reasons that malicious attacks continue to occur at an alarming rate in IoT systems is the poor compliance with information security policies that are mainly caused by behavior issues and the severe lack of security awareness” (p. 3). Identifying the root causes of these “unintentional

insider threats" is critical for enhancing cybersecurity (Burrell, 2024; Khan et al., 2022), as the "human factor" represents either a system's weakest link or strongest defense (Willing et al., 2021). The concept of security fatigue is especially useful in this regard, as it can help shed light on how healthcare staff can unknowingly facilitate a cyberattack.

The "Human Factor" in Cyberattacks

Many cyberattacks against hospitals and healthcare facilities exploit human factors and prey on fatigue among staff members to secure a point of entry. Phishing scams, which involve tricking users to disclose confidential information through seemingly legitimate emails or links, are one of the most common and successful forms of data breaches involving EHRs (Jalali et al., 2020; Lee, 2022; Yeng et al., 2022; Yeo & Banfield, 2022). This strategy is especially effective because the deception is carefully disguised through social engineering, with the messages appearing to originate from coworkers or IT staff (Priestman et al., 2019). In a simulation study of six U.S. healthcare institutions, approximately one in seven (i.e., 14.2%) email messages containing a phishing link were clicked on by hospital staff (Gordon et al., 2019). A similar study of a major Italian hospital showed that the user clicked the link in 18% of the phishing emails that were opened (Rizzoni et al., 2022). Although they do not invoke the concept of security fatigue, these authors nonetheless interpret their findings as suggesting that medical staff rely on "automatic habits" (p. 9) due to workload demands.

Malicious software can also be introduced through corrupted external hardware that is connected to hospital equipment by well-intentioned but unaware healthcare personnel (Bhuyan et al., 2020). As Wasserman and Wasserman (2022) explain:

Physical insertion of malware can be just as potent as phishing. Frequently mentioned in the literature are attacks in which infected USBs, external hard drives, or compact

disks are “accidentally” left in employee parking lots. The expectation is that well-meaning staff members who find the devices will plug them into hospital computers to check the files and identify the devices’ owners. Indeed, in an experiment by the U.S. Department of Homeland Security, sixty percent of its employees who found devices in the parking lot inserted those devices into government computers. This number was higher, 90%, if the device carried a government or contractor logo. (p. 5)

The effectiveness of the “dropped device hack” to exploit kindness or natural curiosity via social engineering extends beyond overburdened healthcare personnel, and research suggests that this strategy can be highly successful in a variety of other contexts as well (e.g., Tischer et al., 2016). The technological threats posed by these attacks are especially potent, since operating systems automatically trust these devices as user input and thus allow any malware to bypass system controls, group policy, and antivirus software (Munyira et al., 2025). While security trainings often warn hospital staff against inserting unknown physical storage devices into network computers, individuals who are distracted or otherwise are under significant cognitive strain may be unlikely to remember these best practices.

Reducing Security Fatigue Among Healthcare Personnel

Although mitigating security fatigue is difficult generally (Stanton et al., 2016), it is particularly challenging among healthcare professionals. Existing training typically ensures a reasonably high level of cybersecurity awareness, but the implementation of best practices can be inconsistent (Alanzi, 2023; Nifakos et al., 2021; Waddell, 2024). In their study of more than 250 staff members across five critical care facilities in Ireland, Hore and colleagues (2024) observed that, beyond deficiencies in knowledge about cybersecurity risks and protocols, factors related to environment and culture were the most important sources of non-compliance—issues that remain underappreciated in existing training programs:

Workload was the most commonly cited barrier to safe cybersecurity behavior. Any cybersecurity intervention should not interfere with people managing their workload, nor should they place an undue burden on an already overworked staff. Critical care staff should be supported to complete cybersecurity awareness and training programs without being unduly overburdened. Creating a positive cybersecurity culture is vital to enhance engagement with any cybersecurity interventions, compliance with recommended cybersecurity practices, and reporting of cybersecurity issues. (p. 6)

Along these same lines, Nobles (2022) concludes that “there is a human factors knowledge gap in cybersecurity” (p. 66) due to inattention to cybersecurity risks that cannot be easily addressed through additional training (see also Willing et al., 2021; Yeng et al., 2021). Recognizing these issues, experts have proposed some recommendations to help curb security fatigue.

The measures most often discussed in the literature involve revisiting the design of security procedures to make them simpler and less redundant. Continuous exposure to complex and repetitive tasks (e.g., system updates, frequent password changes) is particularly burdensome, and scholars advise automating these activities and prioritizing the most strenuous protocols only when the risks are especially high (Cram et al., 2021; Furnell, 2024; Khadka & Ullah, 2025). For instance, Mizrak et al. (2025) suggest that “organizations can maintain security standards by implementing more user-friendly security measures like single sign-on (SSO) or biometric authentication while reducing the strain on employees,” also noting that “limiting security alerts to only those that are critical can prevent employees from feeling overwhelmed by unnecessary notifications” (p. 17). In general, successful socio-technical integration involves aligning software with human decision-making processes, designing systems that explicitly account for human error, and implementing adaptive decision-support systems that help reduce cognitive overload and improve performance in high-stress scenarios (Khadka & Ullah, 2025). As Reeves et al. (2021) explain:

“Before an organization implements a new cyber security process, they should consider several questions. For example, will employees perceive the new process to be restricting their freedom? Will it add to their workload? Will it be problematic if employees begin to tune-out this system or process, and is this likely to occur? If any of these are likely, then the practitioner should consider how they will manage these behaviors, and what the organization can do to minimize the level of reactance, habituation, or other disengagement that may result from the change.” (p. 13)

Several other mitigation efforts that have been highlighted in the literature should be mentioned.

- First, in the development of security protocols, healthcare facilities can leverage the expertise of human factors practitioners, who are trained to improve productivity, streamline performance, and help reduce the unintended consequences that stem from failing to consider how humans ordinarily think and behave (Nobles, 2022).
- Second, even after introducing human-centered cybersecurity improvements that account for degraded performance and human error, staff training should explicitly teach employees how to identify and respond to deception and manipulation tactics through which they may be exploited (Nifakos et al., 2021; Waddell, 2024; Willing et al., 2021).
- Finally, Mizrak and colleagues (2025) highlight the importance of mental health care for medical staff, and they propose that “digital detox initiatives—such as periods where employees are not required to engage with security tasks outside of working hours—can help employees recover from the mental demands of constant security vigilance” (pp. 17-18). Although these efforts may not entirely eliminate security fatigue, a combination of nonintrusive and automated security tasks, meaningful

training, and supportive assistance is most likely to reduce burnout and improve compliance.

Conclusion

Security fatigue represents a significant but often overlooked challenge in maintaining strong cybersecurity within healthcare settings. As this report explains, security fatigue develops gradually as workers face constant demands, repeated warnings, and complex or burdensome security tasks. When combined with heavy workloads, cognitive strain, and the fast-paced environment of modern healthcare, these pressures reduce attention to security protocols and create openings for cyberattacks. Understanding this issue involves recognizing the limits of human attention, decision-making, and motivation—not simply viewing noncompliance as a personal failure among staff members. Insights from social psychology, organizational behavior, and human-factors research reveal that effective cybersecurity must be designed around real human capacities. Reducing unnecessary complexity, automating repetitive tasks, strengthening supportive workplace cultures, and offering better training can all help lower the burden that leads to security fatigue. No single strategy will eliminate the problem entirely, but combining thoughtful system design with realistic expectations can improve security outcomes. Ultimately, addressing security fatigue is not only a technical challenge but a human one, and tackling it is essential for protecting patient data, ensuring organizational resilience, and supporting the healthcare professionals who rely on these systems every day.

References

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy? In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati (Eds.), *Digital privacy* (pp. 363-378). Auerbach Publications.

Ada, Y. R., Chahyadhi, B., Wijayanti, R., Suratna, F. S. N., Widjanarti, M. P., & Fauzi, R. P. (2025). Maintaining occupational health: An analysis of fatigue and safety compliance in construction workers. *Journal of Epidemiology and Public Health*, *10*(2), 252-266. https://doi.org/10.26911/jepublichealth.2025.10.02.11

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46. https://doi.org/10.1145/322796.322806

Alanazi, A. T. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. *Cureus*, *15*(10), Article e47026. https://doi.org/10.7759/cureus.47026

Allen, P. C. (2024). Surviving the storm: The key to cyber resilience and incident response in healthcare. *Healthcare Management Forum*, *37*(1), 26-29. https://doi.org/10.1177/08404704231187103

Alobayli, F., O'Connor, S., Holloway, A., & Cresswell, K. (2023). Electronic health record stress and burnout among clinicians in hospital settings: A systematic review. *Digital Health*, *9*, 1-17. https://doi.org/10.1177/20552076231220241

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. *Applied Sciences*, *11*(19), Article 9183. https://doi.org/10.3390/app11199183

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the

challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*, Article 146. https://doi.org/10.1186/s12911-020-01161-7

Ayala, L. (2016). *Cybersecurity for hospitals and healthcare facilities*. Springer. https://doi.org/10.1007/978-1-4842-2155-6

Baumeister, R. F., & Vohs, K. D. (2007). Self-regulation, ego depletion, and motivation. *Social and Personality Psychology Compass*, *1*(1), 115-128. https://doi.org/10.1111/j.1751-9004.2007.00001.x

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behavior in organisations. In *Proceedings of the 2008 new security paradigms workshop* (pp. 47-58). https://doi.org/10.1145/1595676.1595684

Bhana, A., & Ophoff, J. (2023). Risk homeostasis and security fatigue: A case study of data specialists. *Information & Computer Security*, *31*(3), 267-280. https://doi.org/10.1108/ICS-11-2022-0172

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. *Journal of Medical Systems*, *44*(5), Article 98. https://doi.org/10.1007/s10916-019-1507-y

Burkitt, M., & Hutabarat, D. P. (2023). Overcoming policy fatigue and non-compliance. In S. C. Mukhopadhyay, S. N. A. Senanayake, P. W. C. Prasad (Eds.), *Conference on innovative technologies in intelligent systems and industrial applications* (pp. 525-537). Springer. https://doi.org/10.1007/978-3-031-71773-4_32

Burrell, D. N. (2024). Understanding cognitive and behavioral psychological factors that lead to cybersecurity breaches in healthcare. *RAIS Journal for Social Sciences*, *8*(2), 43-53. https://doi.org/10.5281/zenodo.14210814

Califf, C. B., Sarker, S., & Sarker, S. (2020). The bright and dark sides of technostress: A mixed-methods study involving healthcare IT. *MIS Quarterly*, *44*(2), 809-856. https://doi.org/10.25300/MISQ/2020/14818

CERT Insider Threat Team. (2013). *Unintentional insider threats: A foundational study*. (Technical Note CMU/SEI-2013-TN-022). https://doi.org/10.1184/R1/6585575.v1

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, *44*(6), 752-767. https://doi.org/10.1177/0165551517748288

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, *55*(1), 591-621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Coleman, J. W. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology*, *93*(2), 406-439. https://doi.org/10.1086/228750

Cornejo, G. M. (2025). Assessing cybersecurity dynamics: A comparative analysis of data breaches in urban and rural hospitals in the United States. *Security Journal*, *38*(1), Article 25. https://doi.org/10.1057/s41284-025-00475-3

Costa, D. L. (2017). CERT definition of 'insider threat'—updated. *SEI Blog*. https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*(4), 521-549. https://doi.org/10.1111/isj.12319

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

Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., ... & Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the U.S. *JAMA Network Open*, *6*(5), e2312270-e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The job demands-resources model of burnout. *Journal of Applied Psychology*, *86*(3), 499-512. https://doi.org/10.1037/0021-9010.86.3.499

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

Duckworth, A. L., Milkman, K. L., & Laibson, D. (2018). Beyond willpower: Strategies for reducing failures of self-control. *Psychological Science in the Public Interest*, *19*(3), 102-129. https://doi.org/10.1177/1529100618821893

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. *Journal of Medical Internet Research*, *26*, Article e46904. https://doi.org/10.2196/46904

Feige, E. L. (1999). Underground economies in transition: Non-compliance and institutional change. In E. L. Feige & K. Ott (Eds.), *Underground economies in transition: Unrecorded activity, tax evasion, corruption and organized crime* (pp. 11-27). Ashgate.

Furnell, S. (2010). Usability versus complexity–striking the balance in end-user security. *Network Security*, *2010*(12), 13-17. https://doi.org/10.1016/S1353-4858(10)70147-1

Furnell, S. (2021). Security fatigue. In S. Jajodia, P. Samarati, & M. Yung (Eds.), *Encyclopedia of cryptography, security and privacy* (pp. 2287-2291). Springer. https://doi.org/10.1007/978-3-642-27739-9_1591-1

Furnell, S. (2024). Usable cybersecurity: A contradiction in terms? *Interacting with Computers*, *36*(1), 3-15. https://doi.org/10.1093/iwc/iwad035

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

Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C., & Tariverdi, M. (2021). Assessing resilience of hospitals to cyberattack. *Digital Health*, *7*, 1-15. https://doi.org/10.1177/20552076211059366

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2020). Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal*, *8*(11), 8707-8718. https://doi.org/10.1109/JIOT.2020.3045653

Gofen, A. (2015). Reconciling policy dissonance: Patterns of governmental response to policy noncompliance. *Policy Sciences*, *48*(1), 3-24. https://doi.org/10.1007/s11077-014-9202-9

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., ... & Landman, A. B. (2019). Assessment of employee susceptibility to phishing attacks at U.S. health care institutions. *JAMA Network Open*, *2*(3), e190393-e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

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

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019). Review of security and privacy for the Internet of Medical Things (IoMT). In *15th international conference on distributed computing in sensor systems (DCOSS)* (pp. 457-464). IEEE. https://doi.org/10.1109/DCOSS.2019.00091

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 new security paradigms workshop* (pp. 133-144). https://doi.org/10.1145/1719030.1719050

Hore, K., Tan, M. H., Kehoe, A., Beegan, A., Mason, S., Al Mane, N., ... & Magner, C. (2024). Cybersecurity and critical care staff: A mixed methods study. *International Journal of Medical Informatics*, *185*, Article 105412. https://doi.org/10.1016/j.ijmedinf.2024.105412

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2-18. https://doi.org/10.1108/OIR-11-2015-0358

Jalali, M. S., Landman, A., & Gordon, W. J. (2021). Telemedicine, privacy, and information security in the age of COVID-19. *Journal of the American Medical Informatics Association*, *28*(3), 671-672. https://doi.org/10.1093/jamia/ocaa310

Jancsics, D., Espinosa, S., & Carlos, J. (2023). Organizational noncompliance: An interdisciplinary review of social and organizational factors. *Management Review Quarterly*, *73*(3), 1273-1301. https://doi.org/10.1007/s11301-022-00274-9

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. *American Economic Review*, *93*(5), 1449-1475. https://doi.org/10.1257/000282803322655392

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3), 1-13. https://doi.org/10.1007/s10207-025-01032-0

Khan, N., J. Houghton, R., & Sharples, S. (2022). Understanding factors that influence unintentional insider threat: A framework to counteract unintentional risks. *Cognition, Technology & Work*, *24*(3), 393-421. https://doi.org/10.1007/s10111-021-00690-z

Langer, S. G. (2017). Cyber-security issues in healthcare information technology. *Journal of Digital Imaging*, *30*(1), 117-125. https://doi.org/10.1007/s10278-016-9913-x

Lavanya, P., Raman, V. V., Gosakan, S. S., Glory, H. A., & Sriram, V. S. (2024). Silent threats: Monitoring insider risks in healthcare sector. In V.S. Shankar Sriram, A. G. H. G. Li, & S. R. Pokhrel (Eds.), *International conference on applications and techniques in information security* (pp. 183-198). Springer. https://doi.org/10.1007/978-981-97-9743-1_14

Lee, I. (2022). Analysis of insider threats in the healthcare industry: A text mining approach. *Information*, *13*(9), Article 404. https://doi.org/10.3390/info13090404

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the heuristic–systematic model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38. https://doi.org/10.1016/j.cose.2012.12.003

Makkai, T., & Braithwaite, J. (1991). Criminological theories and regulatory compliance. *Criminology*, *29*(2), 191-220. https://doi.org/10.1111/j.1745-9125.1991.tb01064.x

Martin, A. W., Lopez, S. H., Roscigno, V. J., & Hodson, R. (2013). Against the rules: Synthesizing types and processes of bureaucratic rule-breaking. *Academy of Management Review*, *38*(4), 550-574. https://doi.org/10.5465/amr.2011.0223

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, *358*, Article j3179. https://doi.org/10.1136/bmj.j3179

Martinez-Moyano, I. J., McCaffrey, D. P., & Oliva, R. (2014). Drift and adjustment in organizational rule compliance: Explaining the “regulatory pendulum” in financial markets. *Organization Science*, *25*(2), 321-338. https://doi.org/10.1287/orsc.2013.0847

Millington, T. I., Chilcott, R. P., & Williams, J. (2022). Experiences of personal protective equipment and reasons for non-compliance. *Journal of Paramedic Practice*, *14*(10), 411-418. https://doi.org/10.12968/jpar.2022.14.10.411

Mizrak, F., Demirel, H. G., Yaşar, O., & Karakaya, T. (2025). Digital detox: Exploring the impact of cybersecurity fatigue on employee productivity and mental health. *Discover Mental Health*, *5*(1), 1-21. https://doi.org/10.1007/s44192-025-00149-x

Munyira, A., Kudaro, C. D., Senyonga, H., & Katende, C. (2025). Exploiting the human element: A multivector study on USB attacks, AI-driven phishing, and metadata-based surveillance. *International Journal of Computer Applications*, *187*(56), 29-44. https://doi.org/10.5120/ijca2025925974

Muraven, M., & Baumeister, R. F. (2000). Self-regulation and depletion of limited resources: Does self-control resemble a muscle? *Psychological Bulletin*, *126*(2), 247-259. https://doi.org/10.1037/0033-2909.126.2.247

Neprash, H. T., Dameff, C., & Tully, J. (2024). Cybersecurity lessons from the Change Healthcare attack. *JAMA Internal Medicine*, *184*(11), 1283-1284. https://doi.org/10.1001/jamainternmed.2024.3162

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., ... & Nikpay, S. S. (2022). Trends in ransomware attacks on U.S. hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, *3*(12), Article e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), Article 5119. https://doi.org/10.3390/s21155119

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica Journal of Business and Public Administration*, *13*(1), 49-72. https://doi.org/10.2478/hjbpa-2022-0003

Norton, C., Ruhwanya, Z., & Ophoff, J. (2025). Factors contributing to cybersecurity fatigue. In S. Furnell & N. Clarke (Eds.), *International symposium on human aspects of information security and assurance* (pp. 198-211). Springer. https://doi.org/10.1007/978-3-032-02504-3_14

Palmer, D. (2012). Normal organizational wrongdoing: A critical analysis of theories of misconduct in and by organizations. Oxford University Press.

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2022). A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies*, *33*(6), Article e4049. https://doi.org/10.1002/ett.4049

Parasrampuria, S., & Henry, J. (2019). Hospitals' use of electronic health records data, 2015–2017. *ONC Data Brief*, *46*(1), 1-13.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioral response to emails. In L. J. Janczewski, H. B. Wolfe, & S. Shenoi (Eds.), *IFIP international information security conference* (pp. 366-378). Springer. https://doi.org/10.1007/978-3-642-39218-4_27

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. In N. Clarke & S. Furnell (Eds.), *Proceedings of the tenth international symposium on human aspects of information security & assurance* (pp. 189-198). HAISA.

Perakslis, E. D. (2014). Cybersecurity in health care. *New England Journal of Medicine*, *371*(5), 395-397. https://doi.org/10.1056/NEJMp1404358

Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic impact of a hospital cyberattack in a national health system: Descriptive case study. *JMIR Formative Research*, *7*(1), Article e41738. https://doi.org/10.2196/41738

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*(1), Article e100031. https://doi.org/10.1136/bmjhci-2019-100031

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*, *11*(1), 1-18. https://doi.org/10.1177/21582440211000049

Reeves, K. (2024). Cyberattacks: Not a matter of if, but when. *Applied Radiology*, *53*(2), 38-41.

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health*, *8*, 1-13. https://doi.org/10.1177/20552076221081716

Schnelle, T. (2025). Non-compliance as a determinant of constitutional change? A comparative study. *Constitutional Political Economy*, *36*(3), 376-399. https://doi.org/10.1007/s10602-024-09444-1

Stadin, M., Nordin, M., Fransson, E. I., & Broström, A. (2020). Healthcare managers' experiences of technostress and the actions they take to handle it–a critical incident analysis. *BMC Medical Informatics and Decision Making*, *20*(1), Article 244. https://doi.org/10.1186/s12911-020-01261-4

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

Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A national survey of hospital cyber attack emergency operation preparedness. *Disaster Medicine and Public Health Preparedness*, *17*, Article e363. https://doi.org.10.1017/dmp.2022.283

Sunil, V., & Mathew, S. P. (2024). A systematic review on cybersecurity threats and challenges in hospitals. *Acta Medica International*, *11*(1), 1-6. https://doi.org/10.4103/amit.amit_7_24

Tarafdar, M., Tu, Q., & Ragu-Nathan, A. T. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems*, *27*(3), 303-334. https://doi.org/10.2753/MIS0742-1222270311

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, *10*(3), Article 100549. https://doi.org/10.1016/j.hlpt.2021.100549

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users really do plug in USB drives they find. In *2016 IEEE symposium on security and privacy* (pp. 306-319). IEEE. https://doi.org/10.1109/SP.2016.26

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

Tsai, L. L. (2015). Constructive noncompliance. *Comparative Politics*, *47*(3), 253-279. https://doi.org/10.5129/001041515814709329

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health Security*, *18*(3), 228-231. https://doi.org/10.1089/hs.2019.0123

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication & Society*, *7*(1), 92-114. https://doi.org/10.1080/1369118042000208924

Waddell, M. (2024). Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. *Healthcare Management Forum*, *37*(1), 13-16. https://doi.org/10.1177/08404704231196137

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*, Article 862221. https://doi.org/10.3389/fdgth.2022.862221

Weaver, R. K. (2014). Compliance regimes and barriers to behavioral change. *Governance*, *27*(2), 243-265. https://doi.org/10.1111/gove.12032

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), Article e23692. https://doi.org/10.2196/23692

Willing, M., Dresen, C., Gerlitz, E., Haering, M., Smith, M., Binnewies, C., ... & Schinzel, S. (2021). Behavioral responses to a cyber attack in a hospital environment. *Scientific Reports*, *11*(1), Article 19352. https://doi.org/10.1038/s41598-021-98576-7

Yeng, P. K., Fauzi, M. A., & Yang, B. (2021). Assessing the effect of human factors in healthcare cyber security practice: An empirical study. In *Proceedings of the 25th Pan-Hellenic conference on informatics* (pp. 472-476). https://doi.org/10.1145/3503823.3503909

Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). Investigation into phishing risk behavior among healthcare staff. *Information*, *13*(8), Article 392. https://doi.org/10.3390/info13080392

Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management*, *19*(2), 1-10.

Zadeh, M. M., & Haggerty, N. (2023). Intentional noncompliance: Influencing employees' compliance decision in healthcare services. *International Journal of Healthcare Technology and Management*, *20*(2), 126-143. https://doi.org/10.1504/IJHTM.2023.131519

Author Biography

Peter S. Lehmann, Ph.D., is an Associate Professor in the Department of Criminal Justice and Criminology at Sam Houston State University. His research interests include juvenile justice and delinquency, criminal sentencing, racial and ethnic disparities in punishment, school discipline and safety, and public opinion on crime and criminal justice policy. His published work has appeared in *Justice Quarterly*, *Journal of Research in Crime and Delinquency*, *Crime & Delinquency*, *Punishment & Society*, and other journals.

https://orcid.org/0000-0002-5345-4343

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, Public Health, Water and Wastewater.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute For Homeland Security

Sam Houston State University

Lehmann, P. (2026). Security Fatigue as Insider Threat: Sources, Consequences, and Mitigation. (Institute for Homeland Security Report No. 2026-1032).

Institute for Homeland Security.