RAIS Journal for Social Sciences | VOL. 8, No. 2, 2024
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI: 10.5281/zenodo.14210814

Understanding Cognitive and Behavioral Psychological Factors that Lead to Cybersecurity Breaches in Healthcare

Darrell Norman BURRELL

University of Maryland School of Pharmacy, Baltimore, MD, USA
Marymount University, Arlington, VA, USA
ORCID: https://orcid.org/0000-0002-4675-9544; E-Mail: dburrell@marymount.edu

ABSTRACT: Healthcare institutions are prime targets for cyber-attacks due to their extensive repositories of sensitive patient data and essential operational systems. Human error frequently initiates security breaches in these high-stakes settings, exacerbated by cognitive strain, limited training, and inadequate system design. Research highlights that over 80% of such incidents stem from human-enabled errors, with factors like security fatigue and cognitive overload significantly influencing cybersecurity actions. Despite this, many organizations fail to address the complexities of human behavior in cybersecurity, relying instead on cursory training programs that overlook the nuances of human error. As cybersecurity systems grow more sophisticated, healthcare personnel face increased cognitive and operational demands, further heightening error risks. This study addresses this critical gap by examining the role of human factors psychology in cybersecurity for healthcare and advocating for scientifically grounded strategies that incorporate human behavior, decision-making, and error mitigation to enhance institutional resilience against cyber threats.

KEYWORDS: healthcare cybersecurity, behavioral psychology, human factors psychology, cognitive psychology, human error in cybersecurity, cyberpsychology

Introduction

Research identifies several cybersecurity threats in the healthcare industry, underscoring the sector's vulnerability to increasingly sophisticated attacks (Kruse et al. 2017). One of the primary threats, ransomware attacks, involves cybercriminals breaching healthcare networks, encrypting sensitive files, and demanding a ransom to restore access. Ransomware has caused substantial operational disruptions in healthcare facilities, leading to compromised patient care and financial losses (Kruse et al. 2017). Such attacks leverage elements of criminal psychology, exploiting fear and urgency to pressure victims into paying ransoms, often under severe time constraints. This tactic capitalizes on psychological manipulation to coerce organizations into compliance to avoid data loss or exposure.

Another significant risk factor involves employee-related breaches. Many security incidents stem from human error, where employees inadvertently access malicious files or neglect security protocols (Ncubukezi 2022; Coffey 2017; Algarni et al. 2019; Alsharif et al. 2022). This highlights the need for enhanced training and cybersecurity awareness, as cybercriminals frequently use tactics that manipulate employees' trust or inattention to gain system access. Cyber threats further complicate the landscape, with the healthcare sector experiencing an annual increase of 22% in attacks targeting medical information (Kruse et

al. 2017). These attacks exploit weaknesses in healthcare IT systems, leveraging social engineering techniques like phishing, which play on psychological triggers such as curiosity, urgency, or authority bias (Ncubukezi 2022; Coffey 2017; Algarni et al. 2019; Alsharif et al. 2022).

Human error in cybersecurity often arises from predictable cognitive and behavioral patterns well-documented in human factors psychology, cyberpsychology, cognitive psychology, and behavioral psychology. Key vulnerabilities include phishing and social engineering, where employees inadvertently provide credentials to attackers due to lack of awareness or verification (Hadlington 2018; Triplett 2022). Weak password practices, such as reusing credentials, exemplify how cognitive biases, like prioritizing convenience over security, can lead to vulnerabilities (Nobles 2018; Nobles 2022; Nobles 2019). Cognitive psychology explains behaviors and habits formed around easily memorable or repetitive passwords make users more likely to repeat them across platforms, creating points of entry for attackers (Maalem-Lahcen et al. 2020). Likewise, behavioral psychology suggests that establishing strong password hygiene and implementing multi-factor authentication (MFA) can counteract these tendencies by reshaping users' behaviors through structured security protocols (Hadlington 2018; Triplett 2022). Furthermore, failing to install timely security updates reflects 'cognitive overload and decision fatigue ', a state where individuals may prioritize immediate tasks over seemingly non-urgent system updates, leaving known security gaps unaddressed. Similarly, errors like the miss-delivery of sensitive information, often due to reliance on auto-complete features, highlight how automation and cognitive shortcuts intended to reduce task time can inadvertently expose sensitive data (Hadlington 2018; Triplett 2022).

Other issues, like improper configuration and permissions management, demonstrate how mental processing and oversight errors can lead to excessive access rights, increasing risks for data misuse. Human factors psychology reveal that a lack of routine checks and procedural safeguards can create complacency, especially when individuals rely heavily on automated systems to prevent errors (Nobles 2018; Nobles 2022, Nobles 2019). Behavioral patterns also play a role in neglecting MFA, where employees may avoid MFA for convenience, disregarding security implications. Additionally, unsafe handling of removable media introduces further risks; individuals may overlook the potential of malware transmission due to inadequate training or habitual behaviors around device use (Hadlington 2018; Triplett 2022). Lastly, sharing sensitive data on social media illustrates cyberpsychology tendencies toward information sharing and self-disclosure, where users may underestimate their posts' potential reach and security impact. These examples underscore the importance of a proactive cybersecurity culture, which, when combined with comprehensive cybersecurity training and vigilant policies, can strengthen resilience against human error in healthcare (Hadlington 2018; Triplett 2022).

The psychological insight into criminal behaviors reveals that attackers select targets based on perceived reward and risk assessment; healthcare's high-value data and relatively low defenses increase its attractiveness to cyber criminals. These threats underscore the urgent need for healthcare organizations to adopt advanced cybersecurity strategies, including enhanced employee training, to protect against the evolving tactics and psychological manipulations used in cybercrime (Burrell 2023).

Healthcare institutions are among the top targets for cyber-attacks due to their vast repositories of sensitive patient data and critical operational systems (Burrell 2023; Burrell 2024; Burrell et al. 2023; Burrell et al. 2022; Richardson et al. 2023). Human error is a frequent catalyst for breaches in high-stakes environments, often facilitated by cognitive strain, inadequate training, and flawed system designs. Research reveals that over 80% of breaches result from human-enabled errors, with psychological factors such as security fatigue and cognitive overload significantly impacting employee actions in cybersecurity

operations (Nobles 2018). Unlike popular perceptions, cybersecurity is not a one-size-fits-all solution but rather a multi-layered discipline prone to human and technical vulnerabilities (Ncubukezi 2022; Coffey 2017; Algarni et al. 2019; Alsharif et al. 2022).

Cybersecurity errors carry significant consequences for organizations, including potential data breaches, financial losses, and disruptions to operational continuity (Nobles, 2018; Nobles, 2022). The demand for robust cybersecurity systems intensifies as digital infrastructures become more complex and interconnected. However, many organizations remain vulnerable due to persistent gaps in cybersecurity protocols, insufficient training, and flawed system designs (Nobles 2018; Nobles 2022). These errors stem from a combination of technical and human factors, such as misconfigured systems, inadequate leadership support, and the substantial cognitive demands placed on cybersecurity professionals (Ncubukezi 2022; Coffey 2017; Algarni et al. 2019; Alsharif et al. 2022).

Compounding these challenges is a critical shortage of qualified cybersecurity professionals, which compromises organizations' preparedness and response capacities against mounting cyber threats (Ncubukezi, 2022; Coffey, 2017; Algarni et al., 2019; Alsharif et al. 2022). Effective security hinges as much on addressing human factors as it does on technological defenses (Nobles 2018; Nobles 2022).

Problem Statement

Cybersecurity incidents are increasingly driven by human factors, particularly human error, which research identifies as the predominant cause of data breaches, ransomware attacks, and various cyber threats (Nobles 2018; Nobles 2022). Studies indicate that over 80% of cybersecurity incidents are attributable to human-enabled mistakes, yet organizations often fail to address this problem comprehensively (Nobles 2018). Instead, they frequently resort to superficial training initiatives that do not adequately engage with the complexities of human behavior within cybersecurity contexts (Nobles 2022). As cybersecurity systems become more sophisticated, personnel face heightened risks of cognitive overload, alert fatigue, and operational fatigue, all impairing human performance and amplifying the likelihood of errors (Nobles 2018; Nobles 2022).

Furthermore, a pervasive underappreciation for human factors psychology as a scientific discipline within organizational information technology structures limits the extent to which human behavior is integrated into cybersecurity strategies (Nobles 2018; Nobles 2022). This study seeks to fill this critical gap by examining the influence of human factors psychology on cybersecurity outcomes and advocating for organizational strategies that reflect the complexities of human error, behavior, and decision-making in digital environments.

Significance, Importance, and Novelty of the Inquiry

This inquiry urgently delves into the cyberpsychology and behavioral psychology challenges of addressing human errors in healthcare cybersecurity, a critical yet often overlooked factor in protecting sensitive medical information. The increasing digitization of healthcare systems has significantly improved the accessibility and management of patient data, but it has also introduced heightened vulnerabilities, particularly due to human error. These errors, including mishandling passwords, failure to recognize phishing attempts, and improper system usage, are frequently exploited by cybercriminals, making them a leading cause of cybersecurity breaches in healthcare. This study presents a novel approach by integrating cyberpsychology to understand better the cognitive, emotional, and behavioral factors contributing to these errors. This research is significant because healthcare organizations are increasingly targeted by cyberattacks, with human errors as a primary gateway for these breaches. By addressing the human element, this study underscores the

need for a more integrated approach to cybersecurity in healthcare, combining technological safeguards with interventions to improve cybersecurity awareness and behavioral change among healthcare workers.

Method

This study employs a narrative literature review approach, drawing from human factors psychology and cognitive psychology research across various fields and industries to provide insights into addressing human error cybercrime risks and cybersecurity vulnerabilities specific to healthcare.

The Swiss Cheese Model of Cybersecurity

The healthcare industry's cybersecurity measures are widely seen as lagging behind those of other critical sectors, but there is significant potential for improvement. This vulnerability is exacerbated by the significant value of healthcare data, such as medical records and personal information, which makes the sector a prime target for cybercriminals (Kruse et al. 2017). Human factors psychology and cyberpsychology provide insight into why healthcare lags in cybersecurity compared to industries that have established more robust defenses. Although healthcare organizations invest in technological innovation, cognitive and behavioral factors influence resource allocation decisions, often resulting in insufficient focus on updating and maintaining cybersecurity infrastructure (Burrell 2023; Richardson et al. 2023). Unlike industries where cybersecurity investment aligns closely with technological growth, healthcare often prioritizes clinical technologies over security, creating a cognitive imbalance that weakens overall defenses (Kruse et al. 2017).

Moreover, healthcare organizations frequently fail to adopt effective cybersecurity best practices in other sectors (Burrell 2023; Richardson et al. 2023). Cognitive psychology and behavioral psychology shed light on this discrepancy: a lack of clearly defined cybersecurity roles and insufficient employee training contribute to heightened risk, as staff may lack the skills and awareness needed to counter threats (Kruse et al. 2017). The Swiss Cheese Model offers a framework for understanding these vulnerabilities by illustrating how weaknesses across multiple layers of defense, whether technical, procedural, or human, can align, creating pathways for security breaches (Ebert et al. 2023; Kamoun and Nicho, 2022). Each "slice" represents a defense layer in this model, yet human errors and system design flaws can intersect, producing exploitable vulnerabilities. Behavioral and human factors psychology underscores the need for a strategy that addresses each layer, from user education to system architecture, to minimize the cumulative impact of these vulnerabilities (Nobles 2018). A comprehensive, holistic approach is crucial in addressing the multifaceted nature of cybersecurity in healthcare.

The concept of a Single Point of Failure (SPOF) further emphasizes the importance of balancing technological defenses with human-centered approaches. A SPOF is any critical component whose failure could lead to a complete operational breakdown, a risk heightened when cybersecurity strategies over-rely on technology and neglect human factors (Bkakria et al. 2021; Davis et al. 2016). Mitigating SPOFs requires redundancy, cross-functional collaboration, resilient backup protocols, and behavioral interventions that promote vigilance among staff. These interventions could include regular cybersecurity training, simulated phishing attacks, and clear communication of security policies. Behavioral and human factors psychology inform this resilience strategy by emphasizing that no single element, whether a specific server or an untrained user, should be able to compromise the entire system (Davis et al. 2016). This holistic approach ensures a cybersecurity culture that values technological robustness and human reliability, ultimately enhancing healthcare's resilience against evolving threats.

Fatigue in Cybersecurity

Cybersecurity professionals face various forms of fatigue, which include physical and mental, that significantly impact their ability to detect, analyze, and respond to security threats effectively (Andrade and Yoo 2019). Physical fatigue, resulting from extended hours of threat monitoring and response, diminishes vigilance and slows reaction times. Human factors psychology explain that prolonged physical strain reduces cognitive capacity, leading professionals to overlook crucial details during high-stakes tasks (Gupta et al. 2024; Nobles 2022). Behavioral psychology further suggests that physical exhaustion not only affects individual performance but also undermines team dynamics, as collaborative efforts require sustained attention (Maalem-Lahcen et al. 2020; Cekic 2019). To address these challenges, mandatory breaks and shift rotations could serve as preventive strategies, helping reduce physical fatigue's impact and enhance overall team resilience by ensuring professionals remain attentive and alert.

Mental fatigue is equally pervasive, stemming from the sustained cognitive load required for complex decision-making in cybersecurity (Paul and Dykstra 2017). Insights from cognitive psychology reveal that extended cognitive demands impair both decision-making and attention to detail, leaving professionals more susceptible to cybersecurity errors, including missed alerts and misconfigurations (Gupta et al. 2024; Nobles 2022). Cyberpsychology research further illustrates that under mental strain, even routine security checks can become error-prone as cognitive resources deplete (Aiken,2017; Debb 2021). A practical solution lies in leveraging AI-driven tools to automate repetitive tasks and streamline alert systems, effectively reducing cognitive load and freeing professionals to focus on more complex security threats. By alleviating mental fatigue, these tools enable cybersecurity teams to maintain a higher level of vigilance and accuracy, enhancing overall digital security in demanding environments (Gupta et al. 2024; Nobles 2022; Nobles 2019).

Cognitive Load and Performance Pressure in Cybersecurity

The intense cognitive load and performance pressure inherent in cybersecurity roles are central to error occurrence, often resulting in cognitive and decision fatigue. Cyberpsychology and cognitive psychology research highlights that tight deadlines and high workloads require rapid decision-making, which increases the likelihood of errors such as misconfigurations, missed alerts, and delayed threat responses (Andrade and Yoo 2019; Cekic 2019; Debb, 2021). Cognitive fatigue develops from sustained vigilance, especially in high-stakes environments where precision and speed are essential. Studies on human error indicate that excessive cognitive demands reduce professionals' ability to perform detailed analysis, a skill vital for identifying nuanced or evolving threats (Gupta et al. 2024; Nobles, 2022). Human factors psychology suggests that strategies like task-sharing and decision-support systems can alleviate cognitive fatigue by distributing mental demands, thereby preventing errors that arise from the overwhelming cognitive load (Gupta et al. 2024; Nobles 2022).

Decision fatigue further compounds these challenges, as cybersecurity professionals must make numerous critical decisions daily, from setting firewalls to selecting response tactics during active threats. Behavioral psychology reveals that repeated decision-making can degrade judgment, leading to fatigue-induced lapses in attention and errors (Andrade and Yoo 2019; Cekic 2019). Under the influence of decision fatigue, cybersecurity professionals may shift from proactive to reactive strategies, resulting in rushed, short-term responses rather than carefully considered solutions (Gupta et al. 2024; Nobles 2022). This shift compromises security, as errors often emerge from snap judgments made under mental strain. Addressing cognitive and decision fatigue requires a multifaceted approach, where physical, mental, and emotional fatigue are recognized and mitigated to reduce error rates

(Gupta et al. 2024; Nobles 2022). As cyber threats evolve, managing these human factors remains essential to maintaining effective cybersecurity defenses and protecting digital environments (Gupta et al. 2024; Nobles 2022).

The Evolution of Perspectives on Human Error

The progression from traditional to contemporary views on human error marks a significant shift in understanding accidents and failures in complex systems. Dekker's (2001) research outlines these distinctions, providing a framework that reframes human error as a product of systemic factors rather than isolated individual faults (Dekker 2001). By examining this shift, we gain valuable insights into the role of human factors and cognitive psychology in creating less error-prone, more resilient systems.

From Individual Fault to Systemic Symptom

The traditional or "old view" of human error holds that those accidents primarily stem from human mistakes, positioning human unreliability as the chief threat to otherwise safe systems. This perspective assumes that the system itself is inherently safe and that humans, by nature, introduce risk due to unreliable behavior (Dekker 2001). In contrast, the "new view" reframes human error as a symptom of underlying systemic issues. According to this view, safety is not an inherent system characteristic but is generated through the complex interplay of system elements and contradictions. Human error signals a misalignment or flaw within the broader system rather than a personal failing, suggesting that solutions should focus on addressing these systemic vulnerabilities (Dekker 2001).

From Intrinsic Soundness to Dynamic Complexity

The old view traditionally regards systems as fundamentally sound, assuming that success is an intrinsic property of well-designed systems. This framework protects the system from human error through selective hiring, rigorous training, and strict adherence to protocols, policies, and procedures (Dekker 2001). However, the new view recognizes that systems are inherently complex, containing competing goals and internal contradictions that individuals must constantly manage. This perspective emphasizes that safety is not a given, but something actively created by individuals who navigate these contradictions daily. Rather than being rigidly controlled, systems must be understood as dynamic, with safety emerging from how people adapt to and mitigate inherent risks within these structures (Dekker 2001).

From Categorization to Systemic Analysis

In the old view, human errors are often classified and categorized in ways that lead to individual blame. This perspective encourages a taxonomy of mistakes, focusing on identifying, labeling, and correcting individual actions perceived as failures (Dekker 2001). The new view, however, advocates for a deeper, more nuanced understanding of error. It suggests that errors should not be viewed as isolated incidents but as indications of underlying systemic issues (Gupta et al. 2024; Nobles 2022; Nobles 2019). Rather than assigning blame, this perspective calls for examining the patterns and mechanisms of failure within the broader system, recognizing that errors are part of a complex network of influences and interactions (Dekker 2001). By adopting this systemic approach, organizations can identify root causes and implement changes that support safer and more reliable outcomes (Gupta et al. 2024; Nobles 2022; Nobles 2019).

Implications for Cognitive and Human Factors Psychology

These distinctions underscore a shift from a blame-oriented model to a systemic approach, reflecting cognitive and human factors psychology principles. The new view aligns with cognitive psychology's understanding that human limitations, such as attention capacity and cognitive load, are predictable and should be accommodated within system design (Nobles 2022). Additionally, human factors psychology emphasizes the need to consider environmental and systemic influences on behavior, suggesting that human error can often be traced to flaws within the system rather than individual shortcomings (Gupta et al. 2024; Nobles 2022; Nobles 2022; Nobles 2019). By focusing on these systemic elements, organizations can design workflows, training, and support mechanisms that enhance safety and minimize the impact of human error (Dekker 2001).

In sum, this shift from viewing human error as an individual fault to understanding it as a symptom of systemic flaws reflects a deeper commitment to creating resilient systems (Nobles 2018; Nobles 2019; 2022). It acknowledges that safety is not a static attribute, but a dynamic outcome shaped by interactions within complex environments where human behavior and system structure are interdependent. This perspective encourages continuous learning and adaptation, moving beyond mere blame to foster environments where errors become opportunities for systemic improvement and greater understanding.

Practical Recommendations for Improving Cybersecurity in Healthcare Organizations

Employee Training and Engagement

1. Provide regular, comprehensive training on cybersecurity threats, including recognizing phishing attempts and avoiding malicious files, as most breaches stem from human error (Kruse et al. 2017).
2. Ensure that training is engaging and relevant, helping employees understand the importance of security measures without contributing to fatigue (Nobles 2022).
3. Encourage a culture of continuous learning to improve awareness of human performance and decision-making, helping employees stay vigilant about cybersecurity (Nobles 2018).

Defined Roles and Responsibilities

4. Establish clear cybersecurity responsibilities for staff to enhance accountability and effectively manage security protocols (Kruse et al. 2017).

System Design and Complexity Reduction

5. Design cybersecurity systems emphasizing human capabilities, making them intuitive to reduce user errors (Nobles 2022).
6. Simplify security measures to prevent overwhelming employees, which can lead to non-compliance and increased fatigue (Nobles 2022).
7. Optimize the layout of workspaces to reduce physical strain, ensuring tasks are within comfortable reach to prevent cognitive and physical fatigue (Tropschuh et al. 2022).

Collaboration with Specialists

8. Collaborate with psychologists, cognitive scientists, and human factors experts to analyze and evaluate end-user behavior in cybersecurity operations, improving the understanding and mitigation of human errors (Nobles 2018).

Investment in Cybersecurity Resources and Protocols

9. Avoid over-investing in technology alone; ensure a balanced approach that addresses technological solutions and underlying behavioral and cognitive issues (Nobles 2018).
10. Implement well-defined procedures for regularly updating software to address vulnerabilities and maintain system security (Kruse et al. 2017).

Organizational Culture and Communication

11. Foster a culture emphasizing clinician and employee wellness, ensuring that mental and physical health initiatives are visible and prioritized at all organizational levels (Privitera 2019).
12. Promote an environment where employees can express concerns about security protocols and suggest improvements, reducing frustration and burnout (Nobles 2022).
13. Develop a workplace culture that values well-being, encourages open discussions about workload and stress, and fosters work-life balance (Tropschuh et al. 2022).

Monitoring, Feedback, and Adjustment Mechanisms

14. Monitoring tools like wearable sensors or periodic assessments (e.g., NASA-TLX, Borg Scale) can track mental and physical strain, providing insights for process adjustments (Tropschuh et al. 2022).
15. Periodically evaluate security policies to ensure they remain effective without overly burdensome on employees (Nobles 2022).

Data Breach and Security Incident Preparedness

16. Develop comprehensive response plans to prepare for potential data breaches and minimize the impact of incidents (Kruse et al. 2017).

Workload and Resource Management

17. Leaders should optimize employee cognitive load and manage workloads to prevent mental exhaustion and maintain cognitive and physical well-being (Privitera 2019).
18. Ensure that cognitive, emotional, and physical workloads are balanced and manageable, respecting boundaries between work and personal time (Privitera 2019).
19. Implement job rotation to reduce repetitive strain and provide cognitive variation, helping employees maintain focus and reduce fatigue (Tropschuh et al., 2022).

Strategic Integration of Human Factors Psychology

20. Embed human factors objectives into the organization’s information strategy to effectively address human-related errors (Nobles 2018).
21. Human factors practitioners should be recognized as critical cybersecurity stakeholders and incorporate their expertise into cybersecurity strategy (Nobles 2022).

Physical and Cognitive Support Aids

22. Introduce tools like exoskeletons or lifting aids to reduce physical demands and the risk of injury, supporting employee health and reducing fatigue (Tropschuh et al. 2022).
23. Encourage regular breaks for mental, physical recovery, and strongly encourage that staff take vacation time that includes work e-mail detox periods (Tropschuh et al. 2022).

By adopting these multifaceted recommendations, healthcare organizations can address cybersecurity's human and technical dimensions, fostering a safer, more resilient environment against cyber threats.

Conclusions

In conclusion, mitigating cognitive and human factors in healthcare cybersecurity is essential and requires strategies rooted in human factors psychology, cyberpsychology, cognitive psychology, and behavioral psychology (Andrade and Yoo 2019; Cekic 2019; Debb 2021). Effective management of cognitive load, through simplified protocols and intuitive interfaces, aligns cybersecurity demands with human cognitive capacities, enabling professionals to focus their mental resources on critical tasks (Andrade and Yoo 2019; Nobles, 2022). Additionally, balancing automatic and controlled cognitive processes by automating routine tasks reduces cognitive strain, while structured breaks and task rotation support sustained focus, thus reducing fatigue and error rates (Debb 2021; Nobles 2022).

Organizations must shift mindsets to cultivate a cyber-secure and cyber-aware culture by fostering employees' shared sense of responsibility (Burrell 2024; Burrell 2023). This transformation begins with a comprehensive education that goes beyond basic cybersecurity training, empowering employees to understand the risks and consequences of cyber threats on a personal and organizational level (Nobles 2018). By integrating cybersecurity into the organization's core values and mission of healthcare organizations, employees can see cybersecurity as a shared duty rather than an isolated task for the IT department (Burrell 2024; Burrell 2023). Moreover, ongoing, interactive learning opportunities, such as simulated phishing attacks, real-life case studies, and hands-on workshops, reinforce employees' understanding of how their daily actions impact security (Triplett 2022). Behavioral psychology supports this approach by building habits of caution and vigilance, embedding cybersecurity into routine actions (Maalem-Lahcen et al. 2020). When employees are consistently reminded that even small actions, like password hygiene and secure data handling, are crucial, they are more likely to view cybersecurity as integral to their roles.

Changing organizational culture to prioritize cybersecurity also requires visible leadership commitment and accountability (Burrell 2024; Burrell 2023). Leaders must model cyber-secure behaviors, communicate openly about cybersecurity goals, and provide frequent updates on organizational efforts to enhance security (Burrell 2024; Burrell 2023). This leadership engagement demonstrates to employees that cybersecurity is a top priority, not an afterthought. Additionally, creating feedback channels allows employees to voice concerns, report suspicious activities, or suggest improvements without fear of blame. Recognizing and rewarding secure behavior is a key element that further reinforces a culture where employees feel valued for their contributions to organizational safety. Cyberpsychology insights reveal that positive reinforcement and support systems foster intrinsic motivation, encouraging employees to adopt secure behaviors willingly (Debb 2021). Through these strategic cultural shifts, organizations can create a cohesive, cyber-aware workforce that actively participates in defending against cyber threats.

References

Aiken, Mary. 2017. *The cyber effect: A pioneering cyberpsychologist explains how human behavior changes online.* New York: Spiegel & Grau.

Algarni, Mohammad, Saad Almesalm, and Muntaser Syed. 2019. "Towards enhanced comprehension of human errors in cybersecurity attacks." In *Advances in Human Error, Reliability, Resilience, and Performance: Proceedings of the AHFE 2018 International Conference on Human Error, Reliability, Resilience, and Performance*, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9 (pp. 163-175). Springer International Publishing.

Alsharif, Maher, Shailendra Mishra, and Mohammed AlShehri. 2022. "Impact of Human Vulnerabilities on Cybersecurity." *Computer Systems Science & Engineering* 40(3).

Andrade, Roberto O., and Sang Guun Yoo. 2019. "Cognitive security: A comprehensive study of cognitive science in cybersecurity." *Journal of Information Security and Applications* 48: 102352.

Bkakria, Anis, Reda Yaich, and Walid Arabi. 2021, December. "Secure and robust cyber security threat information sharing." In *International Symposium on Foundations and Practice of Security* (pp. 3-18). Cham: Springer International Publishing.

Burrell, Darrell Norman. 2023. "Cybersecurity in Healthcare Through the 7-S Model Strategy." *Scientific Bulletin* 28(1): 26-35.

Burrell, Darrell Norman. 2024. "Understanding Healthcare Cybersecurity Risk Management Complexity." *Land Forces Academy Review* 29(1): 38-49.

Burrell, Darrell Norman, Sharon L. Burton, Calvin Nobles, Delores Springs, Allison J. Huff, Kim L. Brown-Jackson, Kevin Richardson, Jorja B. Wright, S. Raschid Muller, and Angel J. Jones. 2023. "The managerial ethical and operational challenges of hospital cybersecurity." In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 444-458). IGI Global.

Burrell, Darrell Norman, Amalisha S. Sabie-Aridi, Anton Shufutinsky, Jorja B. Wright, Calvin Nobles, and Maurice Dawson. 2022. "Exploring holistic managerial thinking to manage healthcare cybersecurity better." *International Journal of Health Systems and Translational Medicine (IJHSTM)* 2(1): 1-13.

Cekic, Elvira. 2019. "The Role of Psychology in Enhancing Cybersecurity." Crim. Just. Issues, 271.

Coffey, John W. 2017. "Ameliorating sources of human error in cybersecurity: technological and human-centered approaches." In *The 8th International Multi-Conference on Complexity, Informatics, and Cybernetics*, Pensacola (pp. 85-88).

Davis, John Sanders, Martin C. Libicki, Stuart E. Johnson, Jason Kumar, and Andrew Karode. 2016. *A framework for programming and budgeting for cybersecurity.* Santa Monica, CA: Rand Corporation.

Debb, Scott M. 2021. "Keeping the human in the loop: Awareness and recognition of cybersecurity within cyberpsychology." *Cyberpsychology, Behavior, and Social* Networking 24(9): 581-583.

Dekker, Sidney WA. 2001. "The re-invention of human error." *Human Factors and Aerospace Safety* 1(3):247-265. Retrieved from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0cb8dec29b56ed1635542c4319f1dc9249e99b54.

Ebert, Nico, Thierry Schaltegger, Benjamin Ambuehl, Lorin Schöni, Verena Zimmermann, and Melanie Knieps. 2023. "Learning from safety science: A way forward for studying cybersecurity incidents in organizations." *Computers & Security*, 103435.

Gupta, Vatsla, Ann Rangarajan, and Calvin Nobles. 2024. "Burnout in the Cybersecurity Profession: A Scoping Review." *MWAIS 2024 Proceedings. 20.* https://aisel.aisnet.org/mwais2024/20.

Hadlington, Lee. 2018. "The "human factor" in cybersecurity: Exploring the accidental insider." In *Psychological and Behavioral Examinations in Cyber Security* (pp. 46-63). IGI Global.

Kamoun, Faouzi, and Mathew Nicho. 2022. "A new perspective on the Swiss cheese model applied to understanding the anatomy of healthcare data breaches." In *Research Anthology on Securing Medical Systems and Records* (pp. 726-749). IGI Global.

Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson, and Kyle Monticone. 2017. "Cybersecurity in healthcare: A systematic review of modern threats and trends." *Technology and Health Care* 25(1): 1-10.

Maalem Lahcen, Rachid Ait, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. 2020. "Review and insight on the behavioral aspects of cybersecurity." *Cybersecurity* 3(2020): 1-18.

Manchi, Ganapathi Bhat, Sidde Gowda, and Jaideep Singh Hanspal. 2013. "Study on a cognitive approach to human error and its application to reduce the accidents at workplace." *International Journal of Engineering and Advanced Technology (IJEAT)* 2(6): 236-242.

Ncubukezi, Tabisa. 2022, March. "Human errors: A cybersecurity concern and the weakest link to small businesses." In *Proceedings of the 17th International Conference on Information Warfare and Security* (p. 395).

Nobles, Calvin. 2018. "Botching Human Factors in Cybersecurity in Business Organizations." *HOLISTICA – Journal of Business and Public Administration* 93 (3):71-88. https://doi.org/10.2478/hjbpa-2018-0024.

Nobles, Calvin. 2019. "Establishing human factors programs to mitigate blind spots in cybersecurity." MWAIS 2019 Proceedings, 22.

Nobles, Calvin. 2022. "Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem." *HOLISTICA – Journal of Business and Public Administration,* Sciendo 13 (1): 49-72. https://doi.org/10.2478/hjbpa-2022-0003.

Paul, Celeste Lyn, and Josiah Dykstra. 2017. "Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations." *Journal of Information Warfare* 16(2): 1-11.

Privitera, Michael R. 2019. "Human Factor Based Leadership: Critical Leadership Tools to Reduce Burnout and Latent Error in a Time of Accelerating Change." *Health* 11(09): 1224.

Richardson, Kevin, Darrell Norman Burrell, Horace C. Mingo, Jennifer Ferreras-Perez, Philip Shen, S. Raschid Muller, Dustin Bessette, and Katrina Khanta. 2023. "Exploring Healthcare Cybersecurity Systems in the Age of COVID-19." In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems* (pp. 274-290). IGI Global.

Salim, Hamid M. 2014. "Cyber safety: A systems thinking and systems theory approach to managing cyber security risks." PhD diss., Massachusetts Institute of Technology.

Triplett, William J. 2022. "Addressing human factors in cybersecurity leadership." *Journal of Cybersecurity and Privacy* 2(3): 573-586.

Tropschuh, Barbara, Stefan Brunner, Fabian Dillinger, and Florian Hagemann. 2022. "An approach to analyze human-caused work errors." *Procedia Cirp* 106 (2022): 9-14.