sciendo

Land Forces Academy Review
Vol. XXIX, No. 1(113), 2024

UNDERSTANDING HEALTHCARE CYBERSECURITY RISK MANAGEMENT COMPLEXITY

Darrell Norman BURRELL
Capitol Technology University, Laurel, MD, USA & University of Maryland-Baltimore, School of Pharmacy-Patients Program, Baltimore, MD, USA
dnburrell@captechu.edu

ABSTRACT

It is important to fully comprehend the critical role of the healthcare and public health sector in safeguarding the economy from various threats, including terrorism, infectious diseases, and natural disasters. The private ownership of many healthcare assets underscores the need for enhanced collaboration and information sharing between the public and private sectors. The COVID-19 pandemic has accelerated the digitalization of this sector, leading to a heightened risk of cyber threats. The increasing reliance on emerging technologies such as blockchain, the metaverse, and virtual reality is further exacerbating the cybersecurity landscape, with the projected cost of cybercrime exceeding $10 trillion in 2023 and an anticipated surge to nearly $24 trillion in the next four years. Human error remains the primary cause of cybersecurity incidents, accounting for 95% of reported cases, with insider threats contributing significantly. Despite increased cyber training and risk mitigation efforts, vulnerabilities continue to be rapidly exploited. This paper provides an in-depth analysis of cybersecurity risks in the healthcare sector, drawing on existing literature and theoretical frameworks to highlight the complex challenges in this evolving landscape.

KEYWORDS: risk management complexity, healthcare cybersecurity, critical infrastructure protection, health administration, public health

1. Introduction

The healthcare and public health sector plays a pivotal role in safeguarding the entirety of the economy against an array of threats, including terrorism, infectious disease outbreaks, and natural disasters. Given that most of the sector's assets fall under private ownership and operation, it becomes paramount to emphasize the necessity of fostering collaboration and facilitating the exchange of information between the public and private sectors. These efforts are indispensable in bolstering the resilience of the critical infrastructure within the healthcare and public health domain in the United States.

The COVID-19 pandemic has brought into focus a comprehensive perspective that while medical equipment, medicines, and supplies can save lives, their impact remains contingent upon their swift and effective deployment to those in critical need (Kennedy-Sims, 2021). The repercussions of any delay or obstruction in delivering these vital supplies can be profoundly detrimental to public health, amplifying the situation's urgency (Kennedy-Sims, 2021). Cybersecurity risks pose a

DOI: 10.2478/raft-2024-0004

potential pain point for possible disruptions. To effectively address pandemics and respond to public health emergencies, it is imperative to establish a robust and secure infrastructure for medical providers, public health emergency response operations, and hospital supply chains.

In the United States healthcare landscape, digital technology has emerged as a potent force that can revolutionize clinical outcomes, healthcare logistics, and healthcare delivery practices (Coventry & Branley, 2018). The digital transformation of healthcare has ushered in exponential advancements in capabilities and operational efficiencies, ushering in improvements across domains such as access, care quality, chronic disease management, public health surveillance, and population health (Burrell et al., 2020; Wickham, 2019). Telemedicine technologies facilitate remote care, and electronic health record (EHR) systems streamline data management and medical devices and aid in medication delivery and health monitoring (Coventry & Branley, 2018). However, this rapid digitization also exposed vulnerabilities in cybersecurity, with cyberattacks in the healthcare sector costing the U.S. a staggering 6.2 billion dollars annually, averaging 2.2 million dollars per incident, and resulting in 3,128 records breached on average (Burrell et al., 2020). Notably, there has recently been a substantial 300% increase in cyberattacks targeting the healthcare industry (Janofsky, 2019).

These cyber threats extend beyond data breaches, posing a severe risk to vital healthcare operations. They can compromise laboratory functions, appointment management systems, bed allocation systems, medical devices, medical record management, and the overall organizational capacity of healthcare institutions. Consequently, healthcare privacy and the ability of healthcare organizations to fulfill their mission of delivering high-quality care to patients are jeopardized. The escalating cybersecurity threat, particularly in the context of a global pandemic, underscores the immediate imperative for organizations to adopt a systems-thinking approach to mitigate mass disruption and sustained losses (Burrell et al., 2020). Despite significant investments to shore up cyber defenses, cybersecurity remains an ongoing and critical concern in the healthcare sector in ways that require organizations and leaders to fully understand the complexities of the problem and the risks (Burrell et al., 2020).

Complexity thinking constitutes a comprehensive and dynamic approach aimed at analyzing the intricate interactions among the constituents of a system and how these interactions collectively shape the system as a whole (Nobles, 2018). In stark contrast to reductionist thinking, which perceives the world through a static, simplistic, and one-dimensional lens, systems thinking profoundly emphasizes embracing the system's complexity, dynamism, and entirety. It delves into the interconnections and multifaceted relationships that bind the components of the system together (Nobles, 2018).

Complexity science, an interdisciplinary field, offers a conceptual framework for understanding an array of phenomena characterized as complex and interconnected systems.

Complexity science has demonstrated its potency as a framework within organizational science, permeating areas such as strategic management, organization development, and organizational design (Cummings & Worley, 2014; Dent, 2003; Fogelberg & Frauwirth, 2010; Levinthal & Warglien, 1999; Senge, 2014; Shufutinsky, 2018; 2019; Siggelkow & Rivkin, 2005; Simpson, 2007; Vermeulen et al., 2016). In complexity science, the characterization of a system as "complex" hinges on factors such as the number of system components and the intricate interrelationships and interdependencies among these components (Simon, 1962). The definition of a

component varies based on context and the level of analysis, encompassing entities that can range from individuals, inanimate objects, and departments to entire organizations or organizational factors that exhibit autonomous behavior and engage in interactions with other components (Shufutinsky, 2018; 2019). The notion of interrelatedness underscores the significant influence that components can exert on one another in ways that require system-thinking approaches for these complex problems (Stacey, 2011; Skarzauskiene, 2010).

Senge (2006) delineates systems thinking as a conceptual framework that enables individuals to perceive the complex interconnectedness that defines systems as a whole rather than fixating on individual components. These interactions and relationships extend beyond the confines of technology and equipment, encompassing the interconnectedness between people and their workplace environments. This intricate interplay significantly influences workers' behavior, organizational structures, and operational processes (Senge, 2006). Consequently, healthcare leaders must engage in comprehensive planning, risk management, and response strategies to effectively navigate healthcare cybersecurity's evolving and complex landscape.

2. Problem Statement

The rapid shift in healthcare towards digitalization and connected technologies has been significantly accelerated by the COVID-19 pandemic, resulting in a heightened landscape of cyber risks (Zhadan, 2023). As a consequence of this digital transformation, the impact of cybercrime is projected to escalate dramatically, reaching a staggering $10 trillion in 2023, surpassing the Gross Domestic Product (GDP) of all nations worldwide except for the United States and China (Chamorro-Premuzic, 2023). Moreover, this figure is anticipated to surge even further, nearing the $24 trillion mark within four years (Chamorro-Premuzic, 2023). Despite the longstanding existence of vulnerabilities in the cybersecurity landscape, what is particularly disconcerting is the unprecedented velocity at which these vulnerabilities are being exploited. The primary menace within this context of cybersecurity vulnerabilities remains human error, constituting a staggering 95% of all reported incidents, with a substantial 43% of breaches attributed to insider threats (Zhadan, 2023). This paper aims to delve into the intricacies of cybersecurity risks within the healthcare sector, employing a comprehensive review of existing literature and established theoretical frameworks to shed light on the multifaceted challenges posed by this dynamic and evolving landscape.

3. Research Aims

This research endeavors to employ a contextual review of the literature to investigate the cybersecurity practices of healthcare organizations. Through the lens of complexity thinking, this study seeks to delve into the realm of holistic and dynamic managerial perspectives to enhance cybersecurity management within the healthcare domain.

4. Research Method

This paper thoroughly explores the intricacies and hurdles associated with cybersecurity risk management systems in the healthcare sector, employing a meticulous content analysis of existing scholarly literature. The significance of conducting a content analysis review of the literature lies in its capacity to synthesize disparate concepts, theories, and practices within the evolving realm of research on a specific subject. This synthesis is valuable for practitioners seeking insights and a foundational framework for prospective academic investigations. The study draws upon various databases, including ResearchGate, Academia.edu, Google Scholar, Medline,

Business Source Corporate, ProQuest Business, CINAHL, Nature Journals Online, ICPSR, and ProQuest Health. To navigate this expansive landscape of literature, targeted search terms were utilized, encompassing (a) human factors in cybersecurity, (b) human error in cybersecurity, (c) complexity and its relation to cybersecurity, and (d) cybersecurity within the healthcare context. This multifaceted approach ensures a thorough examination of the subject matter from various angles and sources, enriching the analysis's depth and scope.

5. Review of Literature

Cybersecurity is characterized by an inherent complexity that permeates every facet of an organization's ability to protect itself from potential breaches and risks (Nobles, 2018; Dawson, 2018; Dawson, 2020). This complexity encompasses many security issues and various influencing factors (Nobles, 2018; Dawson, 2018; Dawson, 2020). Cybersecurity is inherently multidisciplinary, encompassing sociology, psychology, and information technology. Security concerns emerge from this interdisciplinary amalgamation and are compounded by the convergence of various factors that can introduce errors, risks, and unmitigated vulnerabilities and potentially culminate in organizational crises (Nobles, 2018; Dawson, 2018; Dawson, 2020).

Moreover, the intricacies within cyberspace are further amplified by the intricate interrelationships between its constituent components (Nobles, 2018; Dawson, 2018; Dawson, 2020). Each component within this complex ecosystem has the potential to interact with or be interdependent upon others across multiple domains. The human element is positioned at the nexus of cyberspace, serving as the interface connecting human systems, organizational systems, and technology (Nobles, 2018; Dawson, 2018; Dawson, 2020). Consequently, the concepts of human-systems integration and sociotechnical systems (Booher & Minninger, 2003; Boyce et al., 2011; Landsburg et al., 2008; Passmore et al., 2019; Trist & Emery, 2005; Walker et al., 2008) assume pivotal roles in shaping the cybersecurity landscape within organizations and driving technological advancement on a broader scale (Shufutinsky et al., 2020; Zoto et al., 2019).

Exploring the literature on human error underscores that errors often manifest due to underlying defects within processes, implying that human error exhibits a degree of predictability and can be anticipated within most processes (Chaiken & Holmquest, 2003). Leape contends that errors stem from flaws in the design and conditions of work environments, which can lead even meticulous, competent, and compassionate healthcare professionals to make errors akin to everyday mistakes but with potentially devastating consequences for patients (Leape, 2000). Recognizing that minor errors or failures can cascade into sentinel events under specific circumstances is essential. Understanding and studying error is approached from two perspectives: the person approach, which attributes blame to the human operator, and the system approach, which acknowledges that errors occur due to systemic or process-related factors (Reason, 2000).

Reason (2000) offers an insightful analogy to elucidate the intricacies of systems, likening them to side-by-side slices of Swiss cheese characterized by defensive layers in a constant state of flux − opening, closing, and shifting their positions. A single hole within these layers does not inherently precipitate an error in most scenarios. Issues or violations are typically identified and mitigated in subsequent layers, averting potential errors. However, when the holes align fortuitously, the trajectory of a violation can circumvent these defensive layers, resulting in the convergence of active failures and latent failures within the system (Reason, 2000).

In healthcare, active failures manifest as unsafe actions committed by individuals in direct contact with patients or integral to the system's functioning. These errors manifest in various forms, ranging from slips, lapses, and fumbles to mistakes and procedural violations (Reason, 2000). The complexity associated with redesigning processes is significantly compounded when different staff members and managers receive disparate directives and priorities from their respective supervisors (Reason, 2000).

To comprehensively grasp the dynamics of errors and institute effective preventive measures, it becomes imperative to address systems' human and technical facets concurrently. These complex dynamics necessitate a holistic system-thinking approach encompassing various elements, including organizational processes, structures, capabilities, behaviors, and environmental factors (Shufutinsky, 2018). By adopting this approach, organizations can foster a more robust understanding of the intricate interplay between these facets and proactively engage in error prevention and risk mitigation.

5.1. Complex Adaptive Systems (CAS)

Complex Adaptive Systems (CAS) theory views organizations, including cybersecurity systems, as complex entities with interconnected components that adapt to their environment. In this context, understanding and managing human error involves recognizing the adaptive nature of cybersecurity and how human actions can affect system behavior.

Complex Adaptive Systems (CAS) provide a valuable framework for understanding the rapidly evolving landscape of cybersecurity, especially in the context of the COVID-19 pandemic and the digital transformation era. CAS refers to systems comprised of numerous interconnected and interdependent components that adapt and evolve in response to changing circumstances (Slangen, 2016; Carter & Perriam, 2021). The shift towards digitalization and the proliferation of emerging technologies have transformed the cybersecurity environment, introducing complexity and unpredictability. CAS elements such as decentralized decision-making, feedback loops, and adaptation to external stimuli can help explain the dynamic nature of cyber risks (Slangen, 2016).

5.2. Resilience Engineering

Resilience Engineering theory emphasizes building resilience into systems to adapt to unexpected events and errors (van der Kleij & Leukfeldt, 2020). It recognizes that human errors are inevitable and focuses on creating systems that can absorb and recover from them without catastrophic failure (van der Kleij & Leukfeldt, 2020).

Resilience Engineering, a concept often applied in high-risk and complex industries, offers valuable insights into managing human error in cybersecurity. At its core, Resilience Engineering recognizes that systems are inherently complex and that errors and failures are inevitable. Rather than focusing solely on preventing errors, it emphasizes the ability of organizations to respond effectively to errors and adapt to changing circumstances. Resilience Engineering principles can be instrumental in cybersecurity, where human error plays a significant role.

One key element of Resilience Engineering is the concept of "work-as-done" versus "work-as-imagined". This concept highlights the distinction between how work is designed and planned (work-as-imagined) and how it is carried out in practice (work-as-done). In cybersecurity, organizations often have well-designed security policies and procedures (work-as-imagined) but may encounter deviations from these plans due to human factors, such as employee behavior or unexpected cyber threats (work-as-done). Understanding this distinction helps organizations recognize

that errors are not solely the result of individual failings but can also be influenced by system constraints and contextual factors (van der Kleij & Leukfeldt, 2020). This perspective can inform the development of more adaptive and resilient cybersecurity strategies that account for the realities of human behavior.

Another crucial element of Resilience Engineering is the concept of "proactive drift management". This complexity concept involves recognizing that, over time, systems and practices can gradually drift away from their intended state (van der Kleij & Leukfeldt, 2020). In cybersecurity, proactive drift management acknowledges that security measures and protocols may deviate from their original design due to various factors, including evolving cyber threats and organizational changes. To address this, Resilience Engineering encourages organizations to continuously monitor and adapt their security practices to align with current realities (van der Kleij & Leukfeldt, 2020). Proactive and multifaceted approaches are necessary to prevent errors and vulnerabilities from accumulating over time and reduce the likelihood of insider threats, often rooted in gradual drifts in security practices.

5.3. Joint Cognitive Systems (JCS)

Joint Cognitive Systems (JCS) theory posits that humans and technology should be considered integrated systems (Willett, 2016). In cybersecurity, this means considering the interaction between human operators and technology and designing systems that account for human limitations and capabilities.

Joint Cognitive Systems (JCS) is a theoretical framework that explores the interaction between humans and technology as interconnected and interdependent systems (Willett, 2016). In managing human error in cybersecurity, JCS provides valuable insights into how human cognition, technology, and the cybersecurity environment influence the overall security posture.

One key element of JCS is the notion of distributed cognition, which recognizes that cognitive processes are not confined to an individual's mind but are distributed across individuals, artifacts, and the environment (Willett, 2016). In cybersecurity, this concept highlights the collaborative nature of managing security incidents. Human operators, security tools, and technology systems collectively contribute to detecting, preventing, and mitigating cyber threats. Understanding how these elements interact and share the cognitive load is crucial for effectively managing human error and improving cybersecurity outcomes.

Another element of JCS relevant to cybersecurity is the idea of cognitive artifacts. These are external tools or technologies that extend and enhance human cognitive capabilities. In cybersecurity, cognitive artifacts may include security dashboards, threat intelligence platforms, and incident response playbooks. By designing and integrating compelling cognitive artifacts into the cybersecurity workflow, organizations can empower their personnel to make more informed decisions and reduce the likelihood of errors (Willett, 2016). Moreover, considering the cognitive aspects of technology design, such as user interfaces and system alerts, becomes vital in minimizing human error and improving overall security.

JCS also emphasizes the concept of mutual adaptation, where humans and technology adapt to each other's capabilities and constraints over time (Willett, 2016). In cybersecurity, this means recognizing that human operators and security systems can learn from past incidents and continuously improve their performance. Organizations should foster a culture of learning and adaptation, enabling cybersecurity professionals to refine their skills and technologies to become more effective in managing threats and preventing errors. This iterative process of mutual adaptation can lead to a more resilient and error-resistant cybersecurity ecosystem (Willett, 2016).

5.4. Cognitive Systems Engineering (CSE)

Cognitive Systems Engineering (CSE) examines how humans interact with complex systems and how their cognitive processes contribute to errors (McNeese et al., 2012). It seeks to design systems that align with human cognition and support error prevention and recovery. Cognitive Systems Engineering (CSE) is a multidisciplinary approach focusing on understanding and designing complex systems to support human cognition and decision-making in high-stakes environments (McNeese et al., 2012). In managing human error in cybersecurity, CSE offers valuable insights into optimizing the interaction between human operators and technology systems to enhance cybersecurity outcomes.

One fundamental element of CSE is the concept of cognitive work analysis (CWA). CWA involves analyzing the cognitive demands placed on human operators within a specific task or domain (McNeese et al., 2012). In cybersecurity, CWA can help identify the cognitive processes and knowledge required for effective threat detection, incident response, and error prevention. By understanding the cognitive work involved, organizations can design user interfaces, training programs, and decision support systems that align with human cognitive capabilities and reduce the likelihood of errors (McNeese et al., 2012).

CSE also emphasizes the importance of cognitive artifacts, tools, and technologies designed to support and augment human cognition (McNeese et al., 2012). In cybersecurity, cognitive artifacts may include security information and event management (SIEM) systems, threat intelligence platforms, and incident response playbooks. These artifacts can assist cybersecurity professionals in processing vast amounts of data, making informed decisions, and mitigating threats. Ensuring that cognitive artifacts are well-designed, user-friendly, and integrated seamlessly into the cybersecurity workflow is crucial for minimizing human errors and improving overall security.

5.5. Human Error Accident Reduction Technique (HEART)

Human Error Accident Reduction Technique (HEART) provides a framework for assessing and managing human error in specific contexts (Evans et al., 2019). This model can help identify potential errors and their consequences. Human Error Accident Reduction Technique (HEART) is a method used to assess and mitigate the risk of human error in complex systems and critical operations (Evans et al., 2019). While HEART is commonly applied in safety-critical industries like aviation and healthcare, its principles can also be relevant to managing human error in cybersecurity. HEART focuses on understanding the factors contributing to human error and employs a systematic approach to reduce the likelihood of errors occurring (Evans et al., 2019).

HEART consists of several vital elements that apply to the complexity of managing human error in cybersecurity. One fundamental aspect is the identification of error-producing conditions or factors. These conditions may include high workload, inadequate training, and unclear procedures in cybersecurity. By pinpointing the specific conditions that can lead to human errors, organizations can implement measures to mitigate these factors and reduce error risks (Evans et al., 2019).

Another element of HEART is the quantification of error likelihood. HEART provides a structured framework for assigning probabilities to different types of human errors (Evans et al., 2019). This step is crucial in assessing the overall risk associated with human actions in cybersecurity. Organizations can use these analysis activities to prioritize areas where error reduction efforts are most needed and allocate resources accordingly (Kayisoglu et al., 2022).

HEART also emphasizes the importance of implementing error-reduction strategies. Once error-producing conditions and probabilities are identified, organizations can develop and implement strategies to prevent or mitigate errors (Evans et al., 2019). In cybersecurity, these strategies include improved training and education, developing user-friendly interfaces and tools, and establishing clear incident response procedures. By systematically addressing the factors contributing to human errors, HEART offers a practical approach to enhancing cybersecurity resilience and reducing the likelihood of insider threats.

6. Conclusions

The onset of the COVID-19 pandemic ushered in widespread disruption across the healthcare sector, presenting multifaceted challenges (Barry & Perlroth, 2020). In addition to grappling with the intricate issues surrounding the need for adequate healthcare capacity and resource allocation, healthcare organizations and academic institutions confronted an elevated landscape of cybersecurity threats amid the pandemic's upheaval (Barry & Perlroth, 2020). Since the advent of the COVID-19 crisis, medical centers globally have been in the crosshairs of intricate and coordinated cyber-attacks (Barry & Perlroth, 2020). Regrettably, healthcare enterprises and medical practices often grapple with resource limitations and expertise deficits when safeguarding against cyber-attacks, leaving them vulnerable to security breaches' enduring operational and financial repercussions (Barry & Perlroth, 2020).

Senge (1990) elucidates the concept of systems thinking as a discipline that enables individuals to perceive the intricacies of interconnected phenomena. It provides a framework for recognizing interdependencies over singular entities, discerning evolving patterns over static snapshots, and identifying holistic entities and potential gaps. In cybersecurity, the significance of systems thinking is amplified due to the prevalent technology-centric approach, which furnishes a defensive and static security environment in contrast to the dynamic behavior exhibited by adversaries (Yan, 2020; Dawson, 2020).

To delve further into this complexity, cyber attackers engage in a spectrum of activities, including vulnerability testing, intelligence gathering, weaponization, and the potential theft of data (Yan, 2020; Dawson, 2018). Simultaneously, cybersecurity teams must navigate the intricate terrain of identifying vulnerabilities, responding to attacks, assessing the repercussions of intrusions, and adapting to the ever-evolving array of challenges and threat mechanisms (Yan, 2020). This process must be revised to maintain linearity and predictability (Dawson, 2018; Dawson, 2020), rendering traditional linear and predictable organizational perspectives needing to be revised in this dynamic cybersecurity landscape.

6.1. Possible Solutions

There are some approaches and solutions that can offer healthcare organizations opportunities to be more proactive in healthcare cybersecurity risks. They include:

6.1.1. Comprehensive Training and Awareness Programs

Healthcare organizations should invest in continuous training and awareness programs for employees at all levels. These programs should educate staff on cybersecurity best practices, data protection policies, and the potential consequences of their actions. Employees should be aware of their critical role in maintaining cybersecurity and preventing insider threats.

6.1.2. User-Friendly Security Measures

Implementing user-friendly security measures can reduce the likelihood of errors. This implementation process

simplifies authentication processes, provides clear and concise security guidelines, and offers user-friendly interfaces for security tools. The goal is to make security practices intuitive and user-centric, reducing the chance of errors due to complexity or confusion.

6.1.3. Role-Based Access Control (RBAC)

RBAC is a strategy that limits system access to authorized individuals based on their roles and responsibilities. Healthcare organizations can implement RBAC to ensure that employees only have access to the information and systems necessary for their job functions. This strategic response minimizes the potential for accidental data exposure or unauthorized actions.

6.1.4. Incident Response Planning

Developing and regularly testing incident response plans is crucial. Healthcare organizations should have protocols to quickly identify, contain, and mitigate cybersecurity incidents, including those caused by human error. Timely and effective responses can minimize the impact of errors and breaches.

6.1.5. Behavioral Analytics

Leveraging behavioral analytics tools can help detect anomalous user behavior. These tools can identify deviations from typical user patterns and alert security teams to potential insider threats or errors. By monitoring user activity, organizations can proactively address issues before they escalate.

6.1.6. Regular Security Audits and Assessments

Regular security audits and internal and external assessments can identify vulnerabilities and areas where human error risks may increase. These assessments can guide organizations in implementing targeted security improvements and ensuring compliance with cybersecurity standards.

6.1.7. Cybersecurity Culture

Fostering a cybersecurity-aware culture is essential. Leadership should set an example by prioritizing cybersecurity and emphasizing its importance to the organization's mission. Encouraging employees to report security concerns without fear of reprisal can help identify and address errors and threats more effectively.

6.1.8. Collaboration and Knowledge Sharing

Healthcare organizations should collaborate with industry peers and share best practices for managing human error risks in cybersecurity. Learning from others' experiences and adopting successful strategies can help organizations strengthen their security posture.

By combining these recommendations, healthcare organizations can better manage the complexity of human error in cybersecurity, reducing the risk of breaches and insider threats while safeguarding patient data and critical systems. Additionally, staying informed about emerging threats and continuously adapting cybersecurity measures is essential in the evolving healthcare landscape.

REFERENCES

Barry, E., & Perlroth, N. (2020). *Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack*. The New York Times, available at: https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

Booher, H.R., & Minninger, J. (2003). *Human systems integration in army systems acquisition* in *Handbook of Human Systems Integration*, 663-698. Available at: https://doi.org/10.1002/0471721174.ch18.

Boyce, M., Duma, K.M., Hettinger, L.J., Malone, T.B., Wilson, D.P., & Lockett-Reynolds, J. (2011). Human Performance in Cybersecurity: a Research Agenda. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 55, Issue 1*, 1115-1119. DOI:10.1177/1071181311551233.

Burrell, D.N., Bhargava, N., Springs, D., Dawson, M., Burton, S.L., Anderson, D.P., & Wright, J.B. (2020). Adopting Organizational Cultural Changes Concerning Whistle-Blowing in Healthcare Around Information Security in the "Internet of Things" World. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), Vol. 4, Issue 1*, 13-28. Doi:10.4018/IJHIoT.2020010102.

Carter, S., & Perriam, J. (2021). Cybersecurity, digital failure, and social harm. *Understanding Digital Societies,* 359-386, SAGE Publications. Available at: https://pure.itu.dk/en/publications/cybersecurity-digital-failure-and-social-harm.

Chaiken, B.P., & Holmquest, D.L. (2003). Patient Safety: Modifying Processes to Eliminate Medical Errors. *Nursing Outlook, Vol. 51, Issue 3: S21-4*. DOI: 10.1016/s0029-6554(03)00097-6.

Chamorro-Premuzic, T. (2023). *Human Error Drives Most Cyber Incidents. Could A.I. Help?* Harvard Business Review, available at: https://hbr.org/2023/05/human-error-drives-most-cyber-incidents-could-ai-help.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas, Vol. 113*, 48-52. Available at: https://www.maturitas.org/article/S0378-5122(18)30165-8/fulltext.

Cummings, T.G., & Worley, C.G. (2014). *Organization development and change*. Mason, USA: South-Western Cengage Learning.

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. Business Information Review, Vol. 35, Issue 2, 60-67. Available at: https://doi.org/10.1177/0266382118773624.

Dawson, M. (2020). Cybercrime: Internet Driven Illicit Activities and Behavior. Land Forces Academy Review, Vol. 25, Issue 4, 356-362. DOI: 10.2478/raft-2020-0043.

Dent, E. (2003). The complexity science organizational development practitioner. *Organization Development Journal*, *Vol. 21, Issue 2*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2297056.

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security, Vol. 80*, 74-89. DOI:10.1016/j.cose.2018.09.002.

Fogelberg, D., & Frauwirth, S. (2010). A complexity science approach to occupation: Moving beyond the individual. *Journal of Occupational Science*, Vol. *17, Issue* 3, 131-139. Available at: https://doi.org/10.1080/14427591.2010.9686687.

Janofsky, A. (2019, October 06). *Smaller Medical Providers Get Burned by Ransomware*. Wall Street Journal, available at: https://www.wsj.com/articles/smaller-medical-providers-get-burned-by-ransomware-11570366801.

Kayisoglu, G., Bolat, P., & Tam, K. (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *The Journal of Navigation*, Vol. *75, Issue* 6, 1364-1388. Available at: https://doi.org/10.1017/S0373463322000534.

Kennedy-Sims, C. (2021). *Supply chain management in level I trauma care facilities: Can it determine patient care delivery and funding?* (Order No. 28539929). Available from ProQuest Dissertations & Theses Global.

Landsburg, A.C., Avery, L., Beaton, R., Bost, J.R., Comperatore, C., Khandpur, R., Malone, T.B., Parker, C., Popkin, S., & Sheridan, T.B. (2008). The art of successfully applying human systems integration. *Naval Engineers Journal, Vol. 120, Issue 1*, 77-107. Available at: https://doi.org/10.1111/j.1559-3584.2008.00113.x.

Leape, L.L. (2000). Institute of Medicine medical error figures are not exaggerated. *JAMA, Vol. 284, Issue 1*, 95-7. DOI: 10.1001/jama.284.1.95.

Levinthal, D.A., & Warglien, M. (1999). Landscape Design: Designing for Local Action in Complex Worlds. *Organization Science, Vol. 10, Issue 3*, 342-357. DOI:10.1287/orsc.10.3.342.

McNeese, M.D., Cooke, N.J., D'Amico, A., Endsley, M.R., Gonzalez, C., Roth, E., & Salas, E. (2012). Perspectives on the role of cognition in cyber security. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 56, Issue 1*, 268-271. DOI:10.1177/1071181312561063.

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *Vol. 9, Issue* 3, 71-88. DOI:https://doi.org/10.2478/hjbpa-2018-0024.

Passmore, W., Winby, S., Mohrman, S., & Vanasse, R. (2019). Reflections: Sociotechnical Systems Design and Organization Change. *Journal of Change Management, Vol. 19, Issue 2*, 67-85. DOI:10.1080/14697017.2018.1553761.

Reason, J. (2000). Human error: models and management. *British Medical Journal, Vol. 320*, 768-770. Available at: https://doi.org/10.1136/bmj.320.7237.768.

Senge, P.M. (2006). *The Fifth Discipline: The Art & Practice of the Learning Organization*. New York: Doubleday.

Senge, P.M. (1990). *The Fifth Discipline: The Art & Practice of The Learning Organization*. New York: Doubleday/Currency.

Senge, P.M. (2014). *The fifth discipline field book: Strategies and tools for building a learning organization*. New York: Crown Currency.

Slangen, R. (2016). *Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations: Why a Complex Adaptive Systems Perspective Contributes to Further Understanding Cyber-risk*. TUDelft, Master Thesis. Available at: http://resolver.tudelft.nl/uuid:3951b6a2-db0c-4e69-8da8-9fa28bc28237.

Shufutinsky, A. (2018). Organizational Assessment of a Biotechnology Firm's Safety, Health, and Environmental Department through an Organizational Development Lens. *International Journal of Interdisciplinary & Multidisciplinary Studies, Vol. 4, Issue* 3.

Shufutinsky, A. (2019). Tribalism and Clone Theory in New Leaders and the Resulting Degradation of Organizational Culture. *Psychology & Behavioral Science International Journal, Vol. 10, Issue 2*: 555788. DOI:10.19080/PBSIJ.2019.10.555788.

Shufutinsky, A., Sibel, J., Beach, Saraceno, A., & Beach, A. (2020). O.D. for Robots? Implications of Industry 4.0 on Talent Acquisition and Development. *Organization Development Journal*, *Vol. 38, Issue* 3, 59-76. Available at: https://www.researchgate.net/publication/343671489_OD_for_Robots_Implications_of_Industry_40_on_Talent_Acquisition_and_Development.

Siggelkow, N., & Rivkin, J.W. (2005). Speed and search: Designing organizations for turbulence and complexity. *Organization Science*, *Vol. 16, Issue* 2, 101-122.

Simon, H.A. (1962). The Architecture of Complexity. Proceedings of the American *Philosophical Society, Vol. 106, Issue 6*, 467-82.

Simpson, P. (2007). Organizing in the mist: A case study in leadership and complexity. *Leadership & Organization Development Journal*, *Vol. 28, Issue 5*, 465-482. DOI:10.1108/01437730710761751.

Skarzauskiene, A. (2010). Managing complexity: Systems thinking as a catalyst of the organization's performance. *Measuring Business Excellence, Vol. 14, Issue 4,* 49-64. DOI:10.1108/13683041011093758.

Stacey, R. (2011). *Strategic management and organizational dynamics: The challenge of complexity to ways of thinking about organizations (6th Edition).* London: Pearson Education Ltd.

Trist, E. & Emery, F. (2005). *Organizational Behavior 2: Essential Theories of Process and Structure*, *169*. New York: Routledge. Available at: https://doi.org/10.4324/9781315702001.

Vermeulen, P., Zietsma, C., Greenwood, R., & Langley, A. (2016). Strategic responses to institutional complexity. *Strategic Organization, Vol. 14, Issue 4*, 277-286.

van der Kleij, R., & Leukfeldt, R. (2020). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24-28, 2019, Washington DC, USA 10,* 16-27. DOI:10.1007/978-3-030-20488-4_2.

Walker, G.H., Stanton, N.A., Salmon, P.M., & Jenkins, D.P. (2008). A review of sociotechnical systems theory: a classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science*, *Vol. 9, Issue 6*, 479-499.

Wickham, M.H. (2019). *Exploring data breaches and means to mitigate future occurrences in healthcare institutions: A content analysis* (Order No. 13861149). Available from ProQuest Dissertations & Theses Global. (2216485062).

Willett, K.D. (2016). *Cybersecurity decision patterns as adaptive knowledge encoding in cybersecurity operations.* Doctoral dissertation, Stevens Institute of Technology.

Yan, D. (2020). *A Systems Thinking for Cybersecurity Modeling*. arXiv preprint arXiv:2001.05734.

Zhadan, A. (2023). *World Economic Forum finds that 95% of cybersecurity incidents occur due to human error*. Cybernews. Available at: https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/.

Zoto, E., Kianpour, M., Kowalski, S.J., & Lopez-Rojas, E.A. (2019). A sociotechnical systems approach to design and support systems thinking in cybersecurity and risk management education. *Complex Systems Informatics and Modeling Quarterly*, *Vol. 18*, 65-75.