Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 18(67) No. 2 – 2025
https://doi.org/10.31926/but.ssl.2025.18.67.2.18

CYBER-PSYCHOLOGICAL SYSTEM FAILURES THAT TRANSLATE DEEP-FAKE AND OTHER SOCIAL ENGINEERING ATTACKS IN WAYS THAT HAMPER ORGANIZATIONAL RESILIENCE

Darrell Norman BURRELL[1]

Abstract: *The convergence of digital deception technologies and cyberattack tactics such as deep fakes presents unprecedented threats to healthcare organizations. These cyber threats exploit psychological vulnerabilities and social engineering techniques, exacerbating the challenge of safeguarding sensitive data and critical infrastructure. In the context of escalating multi-crises, including pandemics, geopolitical instability, and rapid technological disruption, healthcare organizations must adopt a holistic strategic management approach to foster organizational resilience. This inquiry investigates the psychological and social science dimensions of these cyber threats within healthcare settings and explores how strategic management, future thinking, dynamic capabilities, ambidexterity, and multi-dexterity can be leveraged to mitigate risk. The discussion incorporates empirical literature, proposes frameworks for resilience, and underscores the necessity of sophisticated strategic approaches to counteract evolving cybersecurity threats.*

Keywords: *Deep-fakes, Social Engineering, Spear Phishing, Whale Phishing, Cyberpsychology, Cybersecurity, Human Error in Cybersecurity, and Human Factors.*

1. Introduction

Healthcare organizations are increasingly confronted by cyber threats that are as psychologically manipulative as they are technologically advanced. Among the most insidious of these are deepfake-enabled social engineering tactics, such as spear phishing and whale phishing, which exploit not only technical vulnerabilities but also the deeply embedded cultural and cognitive patterns that define healthcare environments (Burrell et al., 2021; Burton et al., 2023; Nobles et al., 2022). These attacks do not merely rely on technological sophistication; they succeed by strategically activating

[1] *Dr. Darrell Norman Burrell*, Marymount University & Georgetown University Pellegrino Center for Clinical Bioethics, corresponding author: dburrell@marymount.edu

psychological triggers, such as authority bias and urgency, especially in high-pressure, hierarchical systems where quick decision-making is normalized (Hadnagy & Fincher, 2021). The incorporation of deepfakes, highly realistic yet artificial audio and video messages, further compounds the risk by injecting false but convincing cues into organizational communication streams, diminishing skepticism and accelerating uncritical compliance (Vaccari & Chadwick, 2020).

Deepfakes impersonate leaders and mirror the structural blind spots of targeted organizations. Avoiding a passive outcome requires reframing resilience as a deliberate, strategic capacity built into the architecture of the healthcare system (Burrell, 2023). Without a fundamental reorientation toward systems thinking, supported by forward-looking governance, interdepartmental coordination, and continuous learning, healthcare organizations will remain exposed to threats that move faster, think smarter, and exploit with surgical precision (AlDaajeh & Alrabaee, 2024; Chatterjee, 2022; Singh et al., 2024). Ultimately, the threat posed by AI-driven deception technologies reveals a deeper truth: that the most dangerous vulnerabilities in cybersecurity are systemic, not singular. Without this transformation, adversaries will continue to outmaneuver institutions designed for predictability in an age defined by disruption (Wright & Burrell, 2023).

1.1. Problem Statement

In an era defined by unprecedented uncertainty, volatility, and complex overlapping crises, from public health emergencies to geopolitical instability and rapid technological disruption, healthcare organizations are under growing pressure to not only withstand shocks but to adapt and thrive through them (Burrell et al., 2021). A significant yet underexplored threat to this resilience is the escalating use of deep-fake technology in cyberattacks. Deep-fakes, synthetic audio and video that imitate trusted figures, are being weaponized in increasingly sophisticated social engineering schemes that target the psychological vulnerabilities of employees. As Avery (2023) notes, 98% of cyberattacks exploit human factors, and Reed (2022) identifies 95% of successful breaches as initiated through spear phishing, an increasingly deep-fake-enabled tactic. These figures point to a critical vulnerability in the human dimension of healthcare cybersecurity.

This problem becomes especially salient in the context of organizational resilience. As medium-sized organizations absorb phishing-related costs averaging $14.8 million annually (Reed, 2022), the capacity to anticipate and neutralize deception-based threats becomes central to both survival and sustainable growth. Despite substantial investments in cybersecurity infrastructure, healthcare systems have failed to incorporate psychological preparedness and human-factor design into strategic resilience planning. This is an area in need of more research to develop practical solutions.

1.2. Significance of the Inquiry

Healthcare personnel are at risk to function effectively in time-sensitive, high-pressure environments due to deep-fakes exploiting cognitive shortcuts, such as trust in authority, urgency perception, and social conformity. Escalating uncertainty caused by intertwined multi-crises, ranging from global pandemics to rapid technological change, healthcare organizations are uniquely vulnerable due to the convergence of high-stakes decision-making and digital interdependence (Burrell, 2023; Wright & Burrell, 2023). When weaponized, these heuristics become entry points for malicious actors, compromising both security and safety (Burrell, 2025; Nobles, 2022). This inquiry holds particular significance as it addresses a critical and underexplored dimension of organizational resilience: the psychological manipulation of employees via deep-fake-based cyberattacks.

1.3. Research Question

The research seeks to bridge a critical knowledge gap that investigates how individuals interpret and respond to deep-fake-enabled social engineering attacks within healthcare organizations.

The core research question guiding this inquiry is: **How can healthcare organizations strategically integrate human factors psychology, organizational systems design, and emerging technological safeguards to mitigate the cognitive and emotional vulnerabilities exploited by deepfake-enabled social engineering attacks?**

1.4. Purpose of the Study

The purpose of this qualitative study is to investigate the psychological mechanisms that shape healthcare employees' responses to deepfake-enabled social engineering threats. Employing a focus group design, the study will examine how individuals across clinical, administrative, and information technology roles perceive, interpret, and evaluate synthetic audio and video communications intended to elicit compliance with fraudulent requests and induce violations of organizational policies. This methodological approach facilitates the collection of rich, contextually grounded accounts, allowing participants to articulate both individual sense-making processes and collectively negotiated interpretations of deceptive stimuli encountered in realistic workplace contexts. Given that the effectiveness of deepfake-based attacks often depends on affective reactions, heuristic decision-making, and social influence dynamics, a qualitative focus group methodology is particularly well suited to capturing the cognitive and emotional processes underlying vulnerability and resistance to such threats.

2. Radical Transformations

Advanced technologies such as artificial intelligence, machine learning, and the Internet of Things (IoT) have fundamentally redefined the threat landscape by enabling

real-time behavioral analysis, automated message generation, and personalized deception strategies (Osamor et al., 2025). These tools allow cybercriminals to exploit both digital infrastructure and human psychology with unprecedented precision (Burrell, 2025). For instance, machine learning algorithms can ingest and mimic legitimate organizational communication styles, while natural language processing enables the construction of persuasive, contextually nuanced messages that evade conventional detection systems. Moreover, compromised IoT devices, often deployed with minimal security, serve as accessible vectors for broader network infiltration, exacerbating systemic vulnerabilities (Schmitt & Flechais, 2024).

Deep-fakes pose a significant threat in phishing scenarios bypassing traditional verification methods and enabling sophisticated social engineering attacks, such as vishing and video-based frauds (Osamor et al., 2025). What distinguishes these modern attacks is their use of publicly available data, especially from social media, to engineer trust and familiarity over time. By mapping relationship patterns and studying interpersonal interactions, attackers fabricate a sense of authenticity, often cultivating trust across multiple digital engagements before executing the final deception (Burrell, 2025; Osamor et al., 2025). This patient, psychologically informed manipulation, represents a shift from opportunistic intrusion to long-term, strategic exploitation. In response, the literature underscores the necessity of a dual-pronged defense strategy that integrates cutting-edge technologies like blockchain and behavioral analytics with human-centered awareness frameworks (Burrell, 2024; Nobles, 2018). Such an approach aligns with the growing demand for strategic ambidexterity and multi-dexterity in resilience planning, where technological robustness must coexist with adaptability, cognitive foresight, and operational agility.

2.1. Authority-Obedience Theory

Authority-Obedience Theory in the workplace explains how employees are inclined to comply with directives from superiors without critical evaluation, often prioritizing hierarchical loyalty over personal judgment (Lyu, 2022). Authority-Obedience Theory, originally rooted in obedience experiments, offers a foundational explanation for how hierarchical organizational cultures become fertile ground for exploitation through social engineering (Burrell, 2024). In highly structured healthcare environments, employees are trained to defer to clinical and executive authority with unquestioned compliance, a behavior pattern that attackers readily exploit (Burrell, 2024). For instance, in a recent whaling simulation, a healthcare finance officer received a video message appearing to come from the hospital CEO, fabricated with deep-fake technology, requesting an immediate wire transfer for “urgent procurement of ventilators.” Without a robust managerial framework to question or verify such requests, the officer, primed by years of institutional obedience, complied without hesitation. As Burrell (2024) highlights, such scenarios illustrate how cybercriminals manipulate hierarchical norms to override rational judgment, particularly in organizations lacking dynamic oversight and proactive risk anticipation.

2.2. Authority bias

Authority Bias in the workplace refers to the tendency of employees to unquestioningly accept information or instructions from individuals in positions of power (Wright et al., 1995; Dai et al., 2022). Authority Bias further complicates this vulnerability by elucidating the cognitive mechanisms through which individuals disproportionately trust and legitimize directives from perceived authority figures (Tversky & Kahneman, 1974). Deep-fake voicemails or impersonated emails bearing official letterheads elicit an automatic trust response, bypassing critical faculties and triggering behavior aligned with institutional loyalty. For example, a spear-phishing email embedded with the signature block and communication style of the Chief Information Officer can lead IT staff to immediately disable access controls under false pretenses. Without the organizational ambidexterity to balance procedural compliance with critical reflexivity, these behaviors go unchecked, resulting in avoidable breaches. As Burrell (2024) notes, this erosion of judgment is not due to individual incompetence but to a structural absence of cognitive resilience mechanisms across the organization.

2.3. Compliance theory

Compliance Theory in the workplace highlights how employees often conform to perceived organizational norms and expectations, especially under pressure from authority figures, which can lead to automatic obedience in situations where critical thinking is essential (Bullée et al., 2015; Bullée et al., 2018; Yaokumah et al., 2020). Compliance Theory further reinforces the systemic nature of these failures by demonstrating how social expectations and institutional norms pressure individuals to conform behaviorally, often at the expense of security. In hierarchical settings like hospitals or academic medical centers, responding promptly to administrative directives is not only encouraged; it is implicitly demanded. Motivated by fear of professional reprimand and a conditioned tendency to comply, the clinician bypasses standard verification and triggers a system-wide breach. Cialdini and Goldstein's (2004) theory demonstrates how compliance is contextually driven by environmental cues and institutional conditioning factors that sophisticated attackers understand and exploit with increasing precision. The strategic failure lies not in the individual decisions made under duress, but in the organization's inability to anticipate and neutralize these human vulnerabilities through multi-system resilience frameworks (Nobles, 2018; Nobles & Robinson, 2024; Burrell, 2023; Burrell, 2024).

3. Methodological Approach

To investigate the psychological and cognitive underpinnings of AI-driven social engineering attacks, particularly those involving deep-fake technologies, this study employed a qualitative research design centered on individual, semi-structured interviews with 16 cybersecurity experts. This methodological choice was deliberate, aiming to elicit in-depth reflections on participants' professional encounters with

sophisticated cyber deception. To participate, each participant were required to have 5 years of cybersecurity experience, an advanced degree, and a professional background and training in either artificial intelligence, cyberpsychology, human computer interaction, or human factors. Rather than quantifying behavior, the study sought to interpret the lived experiences, strategic insights, and contextual knowledge that cybersecurity professionals hold regarding the manipulation of human cognition through emergent technologies. Qualitative inquiry, especially in the form of interviews, is well-suited to uncover complex, subjective, and often tacit dimensions of experience that quantitative metrics alone cannot meaningfully capture.

Data Collection Procedures

An interview protocol was meticulously crafted following a comprehensive review of the cybersecurity and human factors literature and refined through expert consultation with professionals from public health and cybersecurity sectors. The protocol consisted of open-ended questions designed to elicit detailed accounts of participants' experiences with social engineering threats, perceived barriers to mitigation, and insights into system-level vulnerabilities. Interviews were conducted either in person or through encrypted video conferencing platforms, depending on participant preference and logistical considerations. Each session lasted approximately 30 minutes and was audio-recorded, with informed consent, to ensure the precision and integrity of data capture. Verbatim transcription followed, accompanied by detailed field notes documenting non-verbal cues and contextual elements, thereby enriching the dataset with observational nuance.

The data collection questions and results are as follows:

1. **What are the cognitive and emotional mechanics involved in social engineering attacks that make employees susceptible?**

   - **Exploiting authority bias to bypass critical thinking (14 out of 16 participants mentioned this perspective account)**
     Participant 5 stated, "When something looks like it's from your boss or a higher-up, especially with the right tone and urgency, you kind of stop thinking and just do it. I've had emails that looked like they came from our CEO, and even I had to catch myself before I clicked. It's automatic, you don't question authority in those moments."

   - **Triggering urgency to override rational processing (16 out of 16 participants mentioned this perspective)**
     Participant 10 stated, "They always make it sound like you have to act right now. Like, If this isn't done in 10 minutes, we lose the deal or someone's job is on the line. That pressure messes with your head. You feel like you don't have time to think or double-check anything. Attackers use emotional urgency to activate the fight-or-flight response, suppressing deliberative thinking and increasing impulsive decision-making."

- **Leveraging fear of consequence to enforce compliance (16 out of 16 participants mentioned this perspective)**
  Participant 1 stated, "Honestly, the scariest ones are the ones that sound like you're in trouble or about to be. One time, I got a message that said there was suspicious activity on my work account and I needed to reset it immediately. I didn't even think. I panicked and clicked before realizing it was fake."

- **Creating trust through familiarity and personalization (16 out of 16 participants mentioned this perspective)**
  Participant 12 stated, "One email mentioned the name of our department head and even referenced a project we were working on. It felt so legit that I didn't question it until I noticed the sender's email address was slightly off. The familiarity tricks your brain into thinking it's safe."

- **Manipulating empathy and social obligation (16 out of 16 participants mentioned this perspective)**
  Participant 15 stated, "They'll pretend to be a coworker who's stuck or needs a favor. Like, 'Hey, can you help me out? I'm locked out and I'm on a call with a client.' It hits you emotionally, you want to help. That's just human. This shows how social engineering taps into emotional resonance and social norms, such as helping behavior or team loyalty, to override protocol."

- **Inducing decision fatigue during high cognitive load (10 out of 16 participants mentioned this perspective)**
  Participant 7 stated, "After back-to-back meetings and a dozen emails, you stop thinking critically. That's when these things get through. You just want to clear your inbox and move on, so you're more likely to slip up. When people are mentally exhausted, they rely on heuristics and become more prone to decision fatigue, increasing susceptibility to deception."

2. **What are the most effective strategic system approaches that allow organizations to better become equipped to address spear phishing and whale phishing attacks?**

- **Establish cross-functional incident response teams with real-time decision authority. (16 out of 16 participants mentioned this perspective)**
  Interview Participant 16 stated, "You can't just leave it to IT anymore. These phishing emails target finance, HR, and even execs directly. We created a response group that includes someone from every department, and it's made a big difference. Now when something weird hits an inbox, it doesn't fall through the cracks."

- **Implement role-based simulation training tailored to high-risk individuals. (16 out of 16 participants mentioned this perspective).**
  Interview Participant 1 stated, "We ran a fake CEO email to test our C-suite. One of them actually clicked the link. That's when it clicked for us too that executives need training that mirrors the pressure and tone they get in real life. Generic training just doesn't work at that level."

- **Integrate behavioral analytics into phishing detection protocols. (12 out of 16 participants mentioned this perspective).**
  Interview Participant 13 stated, "What helped us was using behavioral data, if someone suddenly accesses email at 2 a.m. from a location they've never been to, the system flags it. That, paired with user education, creates this two-layer net that's caught a few close calls."

- **Foster a blame-free reporting culture to encourage rapid detection. (9 out of 16 participants mentioned this perspective).**
  Interview Participant 3 stated, "At first, people were scared to report phishing emails because they thought they'd get in trouble. Once leadership made it clear that reporting was the right move, even if you clicked, we saw incidents being flagged way earlier."

3. **What are the best practices for protecting organizations against deep-fake social engineering attacks?**

- **Establish a deep-fake verification protocol for executive communications. (15 out of 16 mentioned this perspective).**
  Interview Participant 2 stated, "We had to put a policy in place that says any request involving money or access has to be verified via a separate secure channel, even if it looks and sounds like our CFO. Deep-fakes are that good now; you can't trust your eyes or ears anymore."

- **Train staff using real-world deep-fake scenarios with emotional hooks. (11 out of 16 mentioned this perspective).**
  Interview Participant 12 stated, "The first time we showed our team a fake video of our CEO asking for urgent action, people were stunned. It looked so real. That kind of training really hit home because it showed how easily we could be tricked by something that feels legit."

- **Invest in AI-powered content authentication tools. (16 out of 16 mentioned this perspective).**
  Interview Participant 4 stated, "We're using software that scans video and audio for subtle signs of manipulation, stuff the human eye misses. It's not foolproof,

but it adds another layer of protection, especially when paired with awareness training."

- **Create internal communication norms that limit vulnerability. (16 out of 16 mentioned this perspective).**
  Interview Participant 8 stated, "Now our execs don't ask for wire transfers or credit card payments over email or voicemail, period. If you get a message like that, you know it's fake. Just having that rule in place cuts out a lot of confusion and makes deep-fake attempts easier to spot."

4. What are the best approaches to the use of human factors and human error psychology to address social engineering attacks that use deep-fakes?

- **Normalize hesitation and encourage verification as a routine habit. (16 out of 16 mentioned this perspective).**
  Interview Participant 9 stated, "We told our staff it's okay to take five extra minutes to double-check something, even if it feels urgent. Giving people that permission changed the game. They're not afraid to question things anymore, and that's exactly what attackers don't want."

- **Use cognitive bias training to build awareness of authority and urgency manipulation. (9 out of 16 mentioned this perspective).**
  Interview Participant 6 stated, "Once people learned about how attackers use things like authority bias or fear of consequences, you could see the lightbulb go on. One guy said, 'That's exactly why I almost responded to that fake email. I thought I was gonna get fired if I didn't.'"

- **Reduce cognitive overload by streamlining security protocols. (9 out of 16 mentioned this perspective).**
  Interview Participant 2 stated, "We simplified our login and access rules because people were juggling too many steps and making mistakes. Less friction means fewer errors, and it frees up their brainpower to notice when something feels off."

- **Implement routine debriefs after security incidents to reinforce learning. (16 out of 16 mentioned this perspective).**
  Interview Participant 15 stated, "After every incident, even near-misses, we do a no-blame debrief. One staffer said, 'I thought I messed up big time, but talking through it helped me realize what I missed and how to catch it next time.' It's become one of our best learning tools."

4. Conclusion

The proliferation of deep-fake-enabled social engineering attacks in healthcare settings exposes critical system-level vulnerabilities that cannot be addressed through isolated technical solutions alone. Healthcare organizations, which operate as complex adaptive systems, are particularly susceptible to cyber threats that exploit the interplay between cognitive behavior, technological infrastructure, and hierarchical communication channels (Burrell, 2023).

To foster true organizational resilience, healthcare systems must adopt a systems-based cybersecurity framework, one that embeds behavioral training, adaptive feedback mechanisms, and strategic foresight into operational and cultural design (Burrell, 2023). Such resilience is not achieved through static compliance but through systemic reconfiguration: normalizing hesitation, decentralizing decision-making in cyber crises, and institutionalizing psychological safety through continuous learning (Nobles, 2018; Nobles & Robinson, 2024). Only by evolving into cognitively aware and structurally agile systems can healthcare organizations withstand the escalating complexity of cyber threats shaped by artificial intelligence and social engineering.

References

AlDaajeh, S., & Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security*, *141*, 103845.

Alghamdi, A. (2022). A Systematic Review on Human Factors in Cybersecurity. *International Journal of Computer Science & Network Security*, *22*(10), 282-290.

Avery, C. (2023, November 8). *The Impact of AI on Social Engineering Cyber Attack. Secureworld*. Retrieved from: https://www.secureworld.io/industry-news/impact-ai-social-engineering-attacks

Bass, B. M., & Riggio, R. E. (2006). *Transformational leadership* (2nd ed.). New York: Psychology Press.

Brink, H. I. (1993). Validity and reliability in qualitative research. *Curationis*, *16*(2), 35-38.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of experimental criminology*, *11*, 97-115.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks, A literature-based dissection of successful attacks. *Journal of investigative psychology and offender profiling*, *15*(1), 20-45.

Burrell, D. N. (2024, November). Exploring the Cyberpsychology and Criminal Psychology of Whaling and Spear Fishing On-line Attacks. In *RAIS Conference Proceedings 2022-2024* (No. 0465). Research Association for Interdisciplinary Studies.

Burrell, Darrell Norman. (2023). Cybersecurity in Healthcare Through the 7-S Model Strategy. *Scientific Bulletin-Nicolae Bălcescu Land Forces Academy* 28(1), 26-35.

Burrell, D. N. (2025, April). Mental Health Impacts of Cybercrime. In *Proceedings of the 19th International Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited.

Burrell, D. N., Aridi, A. S., McLester, Q., Shufutinsky, A., Nobles, C., Dawson, M., & Muller, S. R. (2021). Exploring system thinking leadership approaches to the healthcare cybersecurity environment. *International Journal of Extreme Automation and Connectivity in Healthcare (IJEACH)*, *3*(2), 20-32.

Burton, S. L., Burrell, D. N., Nobles, C., & Jones, L. A. (2023). Exploring the nexus of cybersecurity leadership, human factors, emotional intelligence, innovative work behavior, and critical leadership traits. *Scientific Bulletin-Nicolae Bălcescu Land Forces Academy*, *28*(2), 162-175.

Caci, L., Nyantakyi, E., Blum, K., Sonpar, A., Schultes, M. T., Albers, B., & Clack, L. (2025). Organizational readiness for change: A systematic review of the healthcare literature. *Implementation Research and Practice*, *6*, 26334895251334536.

Chatterjee, S. (2022). The Critical Role of Change Management in Safeguarding Cybersecurity in Production Environments. *J Artif Intell Mach Learn & Data Sci*, *1*(1), 2089-2096.

Coker, J (2025, March 11). 95% of Data Breaches Tied to Human Error in 2024. *Information Security Magazine*. Retrieved from: https://www.infosecurity-magazine.com/news/data-breaches-human-error/

Dai, Y., Li, H., Xie, W., & Deng, T. (2022). Power distance belief and workplace communication: The mediating role of fear of authority. *International journal of environmental research and public health*, *19*(5), 2932.

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, *134*, 103435.

Engelseth, P., & Kritchanchai, D. (2018, April). Innovation in healthcare services–creating a Combined Contingency Theory and Ecosystems Approach. In *IOP Conference Series: Materials Science and Engineering* (Vol. 337, No. 1, p. 012022). IOP Publishing.

Fried, B. J. (1988). Power acquisition in a health care setting: an application of strategic contingencies theory. *Human Relations*, *41*(12), 915-927.

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PloS one*, *15*(5), e0232076

Hadnagy, C., & Fincher, M. (2021). *Human hacking: Win friends, influence people, and leave them better off for having met you*. Harper Business.

Kelly, P., Hegarty, J., Barry, J., Dyer, K. R., & Horgan, A. (2017). A systematic review of the relationship between staff perceptions of organizational readiness to change and the process of innovation adoption in substance misuse treatment programs. *Journal of Substance Abuse Treatment*, *80*, 6-25.

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on employees. *Journal of Financial Crime*, *23*(3), 612–627. https://doi.org/10.1108/JFC-11-2015-0061

Lehman, W. E., Greener, J. M., & Simpson, D. D. (2002). Assessing organizational readiness for change. *Journal of substance abuse treatment*, *22*(4), 197-209.

Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.

Lyu, L. (2022, July). A Study of the Relationship Between Job Insecurity and Obedience to Authority, The Moderating Role of Psychological Capital. In *2022 3rd International Conference on Mental Health, Education and Human Development (MHEHD 2022)* (pp. 671-675). Atlantis Press.

Miller, M., & Holley, S. (2022). Assessing human factors and cyber attacks at the human-machine interface: Threats to safety and pilot and controller performance. *Human Factors in Cybersecurity*, *53*(53).

Mwita, K. (2022). Factors influencing data saturation in qualitative studies. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(4), 414-420.

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

Nobles, C., Robinson, N., Cunningham, M., Robinson, N., Cunningham, M., & Cunningham, M. (2022, September). Straight from the human factors professionals' mouth: The need to teach human factors in cybersecurity. In *Proceedings of the 23rd Annual Conference on Information Technology Education* (pp. 157-158).

Nobles, C., & Robinson, N. (2024). 3 The benefits of human factors engineering in cybersecurity. *Cybersecurity Risk Management: Enhancing Leadership and Expertise*, 53.

Olden, P. C. (2016). Contingency management of health care organizations: It depends. *The health care manager*, *35*(1), 28-36.

O'Reilly, C. A., & Tushman, M. L. (2013). Organizational ambidexterity: Past, present, and future. *Academy of Management Perspectives*, *27*(4), 324–338. https://doi.org/10.5465/amp.2013.0025

Osamor, J., Ashawa, M., Shahrabi, A., Phillip, A., & Iwend, C. (2025). The Evolution of Phishing and Future Directions: A Review. *Proceedings of the 19th International Conference on Cyber Warfare and Security* 20(1), 361-368. Academic Conferences and publishing limited.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2015). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, technology & work* (Online), *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pollock, T. (2023). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). KSU Proceedings on Cybersecurity Education, Research and Practice. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1051&context=ccerp

Reed, C. (2022, May 9). *10 Eye-Catching Spear Phishing Statistics – 2022. Firewall Times*. Retrieved from: https://firewalltimes.com/spear-phishing-statistics/

Salim, H. M. (2014). *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks* (Doctoral dissertation). Massachusetts Institute of Technology).

Shabani, T., Jerie, S., & Shabani, T. (2024). A comprehensive review of the Swiss cheese model in risk management. *Safety in Extreme Environments*, *6*(1), 43-57.

Schein, E. H., & Schein, P. A. (2017). *Organizational culture and leadership* (5th ed.). Wiley.

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12), 1-23.

Singh, G., Tiwari, D., Goel, P., Vishwakarma, P., Gupta, K., & Verma, A. (2024, May). Cybersecurity Challenges in Healthcare Systems. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 1-6). IEEE.

Statistica (2024) https://www.statista.com/statistics/1417720/worldwide-cost-per-record-by-initial-attack-vector/

Ștefan, S. C., Popa, I., & Tărăban, I. (2023). Strategic orientation of Romanian healthcare organizations from a contingency theory perspective based on Porter's generic strategy model. *Systems*, *11*(10), 488.

Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. Irwin/McGraw-Hill.

Teece, D. J., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility. *California Management Review*, *58*(4), 13–35. https://doi.org/10.1525/cmr.2016.58.4.13

Teece, D. J., Pisano, G., & Shuen, A. (1997). *Dynamic capabilities and strategic management*. Strategic Management Journal, 18(7), 509–533.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319–1350.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Vaccari, C., & Chadwick, A. (2020). Deep-fakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, *6*(1), 2056305120903408. https://doi.org/10.1177/2056305120903408

Von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. New York: George Braziller.

Wright, E. O., Baxter, J., & Birkelund, G. E. (1995). The gender gap in workplace authority: A cross-national study. *American sociological review*, 407-435.

Wright, J., & Burrell, D. N. (2023). Telemedicine Cybersecurity Protection in Reproductive Healthcare. *HOLISTICA Journal of Business and Public Administration*, *14*(2), 1-14.

Yaokumah, Winfred, Muttukrishnan Rajarajan, Jamal-Deen Abdulai, Isaac Wiafe, and Ferdinand Apietu Katsriku (Eds). (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance*. IGI Global.

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in health information management*, *19*(Spring), 1i. Retrieved from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/