Human Factors in Cyber Security

Whitney B. Carpenter

Charleston Southern University

CSCI 405 Principles of Cyber Security

Dr. Patrick Hill

October 21, 2025

Abstract

Humans continue to be the most unpredictable and influential factor in cybersecurity. Most breaches are ultimately caused by human decisions, miscommunications, and organizational weaknesses, not system flaws. This paper will explore cybersecurity through a human-centered lens, showing how cognitive limitations, operational stress, and cultural dynamics affect defense effectiveness. Specifically, it will examine behavioral vulnerabilities among users, human performance issues within security operations, and the crucial role of leadership and culture in shaping collective security breach behavior. Findings show that usability, communication, and psychological safety are just as vital to security as firewalls or encryption. The paper will conclude by outlining a human-centered cybersecurity model that aligns systems, policies, and culture with how people actually think and work, transforming security from reactive protection to proactive resilience.

Keywords: cybersecurity, human factors, usability, organization, culture, behavior, resilience

Human Factors in Cyber Security

Humans are not perfect. Despite all the progress we have made, socially and technologically, humans are still the most unpredictable, and sometimes the weakest, link in cybersecurity systems. Often, security breaches are traced back to human decisions, miscommunications, and systemic stressors, rather than technical flaws. Knowing that, we can understand that cybersecurity is not solely a technical problem, but a human one. By understanding human behavior, work environments, and organizational culture, organizations can design systems and policies that align with how humans actually think and work rather than how they are expected to.

Cognitive and Behavioral Vulnerabilities

Usability and the Limits of Compliance

It is very common for organizations and developers to see users as an obstacle to security, and we see that in the strict or confusing policies that push users toward insecure behavior (Adams & Sasse, 1999). This behavior could be something like writing down passwords, or bypassing systems because they seem too complex. Users should be seen as collaborators, not obstacles, as Adams and Sasse (1999) said, "Users are not the enemy." We need to push for usable security design, because that will allow people to act securely without added cognitive strain.

Manipulation and Deception Cues

Because we are human, we are going to experience human emotions and weaknesses. For example, people are more likely to click malicious links when they are emotionally triggered or they are multitasking and their focus isn't wholly on what it should be. One journal states, "Phishing remains effective because attackers exploit cues such as urgency, authority, and

trustworthiness in design," (Butavicius et al., 2022). Threats that wouldn't normally be as big of a problem could be made more drastic due to the manipulation of human tendencies.

Behavioral Science as Prevention

It has been proven that behavioral science can teach us how to enforce good behavior, and it would be a great avenue to prevent these exploitations of human factors. According to Pfleeger & Caputo (2012), "People behave securely when systems are designed to make secure choices the easiest choices," which means that we need to encourage security by making it simple. Some behavioral approaches that would help encourage this are feedback, reinforcement, and social modeling (Pfleeger and Caputo, 2012). Each of these approaches would make it easier for users and developers to go down the right path and not be strayed by human weaknesses.

Human Factors in Security Operations

Cognitive limitations explain individual vulnerability, but secure performance also depends on how professionals and teams interact with broader systems.

Design and Communication Failures

Even if an organization has the most secure technical safeguards, they will still fail when people do not communicate well. It is even stated that "Most security failures are due not to cryptographic weaknesses but to misunderstandings between system designers, implementers, and users," (Anderson, 2020). This makes it clear that security designers must integrate human testing and cross-disciplinary collaboration. When a team communicates well, and everyone is aware of what is going on in the system as a whole, gaps and vulnerabilities are much less likely to form. Another important factor is communication after an incident; the discussion needs to focus on encouraging learning rather than blaming (Anderson, 2020).

Stress, Fatigue, and Attention

Of course, we all know that when someone is tired, overloaded, or stressed, they are not going to perform their best. That is also the case in cyber security. Overloaded analysts are more likely to miss alerts or misjudge anomalies, so "Human behavior must be treated as an assurance factor; fatigue and workload directly affect security performance" (Evans et al., 2019). Team dynamics, support systems, and mental health support are helpful to mitigate burnout and error, but automation is something that could lighten the load on someone as well. When designing a system, human behavior cannot be ignored, as it directly affects the design.

Operational Evidence of Human Factors

According to Verizon (2024), "Human error continues to be the leading cause of breaches, accounting for 68% of incidents." Misconfigurations, privilege misuse, and missed alerts are operational reflections of human limitations under stress or bad communication. This data shows that most technical incidents have underlying causes of human factors. Human factors like workload balance and communication efficiency should be assessed alongside traditional security measures in order to have sufficient security.

Insider Threats and Predictive Modeling

When inside threats occur, teams tend to have hindsight bias where they can remember all the signs, but they did not recognize them at the beginning. However, insiders often show behavioral signs like stress, disengagement, or sudden rule-breaking, that technical tools alone miss (Greitzer & Frincke, 2010). Implementing predictive modeling, like data-driven baselines, allows for early, ethical intervention, that you couldn't get if you only looked at and used technical data.

Organizational Culture and Leadership

Operational vulnerabilities show that even well-trained professionals are influenced by human limits, so the next level of defense involves cultivating a strong culture, communication, and leadership.

Communication and Role Clarity

When organizations do not have clear roles and communication, there is a significantly higher risk of incidents. Everyone in an organization needs to know their purpose in the design, so they get what they need to done, and so they can communicate that with others. In order to reduce misunderstandings and support secure decision-making, leadership and management must communicate well and have clarity with the technical staff (Nifakos et al., 2021).

Building a Security Culture

Every design team and organization needs to have an open and honest security culture where recognition and transparency are used to foster learning and engagement. It has been proven time and time again that fear and punishment reduce transparency and increase concealment of errors. Another thing that helps build a good culture is moving past just compliance, and focusing on shared responsibility (Pfleeger & Caputo, 2012). Team leaders need to encourage collaboration and honesty over individual blame if they want to have a mature security culture.

Integrating a Human-Centered Cybersecurity Model

Aligning Technology with Human Behavior

To reduce incidents caused by human error, user interfaces should be simplified, behavioral nudges should be applied, and policies need to fit cognitive reality. Sometimes usability gets put on the back burner, but usability testing should be implemented early in the security system design process. Another way to align technology with human behavior is to

integrate education and feedback within software tools, like adding password strength suggestions to a login page or a password checker. Overall, it is important that developers design from the user's perspective.

Supporting Team Members

Just as users need to be treated well, the technicians need to be treated as humans rather than just tools. To do this, organizations should incorporate workload management, communication training, and team resilience programs (Evans, et al., 2019). Organizations often have technical training throughout and in between designs and adding social and communication skills into this training would benefit the team so much.

Lead Through Culture

A culture of adaptive learning, open communication, and extensive collaboration needs to be developed if an organization wants a secure system. A way to ensure that this is working is to hold culture audits to identify communication breakdowns or stress indicators early. A culture of support and security leadership treating people as integral parts of the system and not unpredictable variables to be controlled are the best things that could happen to an organization in terms of security.

Conclusion

As this paper attempts to convey, technology is not the only thing that determines cybersecurity success or failure. Human behavior, as we have learned, is responsible for over half the cyber breaches that have occurred. Understanding the human factors that lead to vulnerabilities and how they can be mitigated is crucial to having a secure system. When a design understands and incorporates human factors, cybersecurity is changed from reactive

defense to proactive resilience. The future of cybersecurity lies not in smarter machines, but in smarter integration of human insight.

References

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

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2022). Why people keep falling for phishing scams: The effects of leakage cues and deception indicators. *Computers in Human Behavior, 133*, 107255. https://doi.org/10.1016/j.chb.2022.107255

Evans, M., Maglaras, L., He, Y., & Janicke, H. (2019). Human behaviour as an aspect of cybersecurity assurance. *Security Journal, 32*(4), 1–20. https://doi.org/10.1057/s41284-019-00173-4

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In M. Bishop & S. Frincke (Eds.), *Insider threats in cyber security* (pp. 85–113). Springer. https://doi.org/10.1007/978-1-4419-7133-3_5

Nifakos, S., Anttila, V., & Wihlborg, E. (2021). Influence of human factors on cyber security within organizations: A systematic review. *Frontiers in Psychology, 12*, 639578. https://doi.org/10.3389/fpsyg.2021.639578

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Verizon. (2024). *Data breach investigations report (DBIR)*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/