

Article Review Paper

Nicholas Duggins

ODU

08/02/2026

Article Review Paper

Introduction

Cybersecurity is far too often treated as a purely technical problem solved by software, firewalls, and complex passwords. However, the reality is that most successful cyberattacks succeed because criminals exploit human psychology rather than breaking raw code. People commit cybercrimes for a variety of complex social and economic reasons, including financial gain, revenge, status, or pure entertainment. At the same time, institutions are left exposed not just by outdated systems, but by human error, high stress levels, weak policies, and unhealthy workplace cultures.

This paper reviews four scholarly articles that approach cybersecurity through a social science lens. By examining workplace dynamics, cognitive strain during cyber threats, institutional policy gaps, and youth participation in cybercrime, these studies demonstrate that human behavior is both the primary vulnerability and the strongest defense in modern cybersecurity.

Article Reviews

1. Ghaleb (2025)

Ghaleb's study explores the organizational dynamics that influence whether employees actually comply with information security policies (ISPs). The central research question examines how cybersecurity awareness, organizational culture, and trust in management work together to predict employee compliance behavior. To test this, the author used a quantitative, cross-sectional survey design, collecting data from 261 employees across various departments. Using statistical modeling (specifically structural equation modeling and regression analysis), the study evaluated how strongly leadership trust and workplace environment impacted rule-following behaviors.

This research strongly reflects several fundamental social science principles. First, it relies on determinism, demonstrating that employee non-compliance isn't just random laziness, but is directly caused by external social conditions like poor workplace culture or low trust in management. It also

demonstrates empiricism through its reliance on statistical survey data rather than guesswork, and relativism by showing that security compliance shifts depending on an organization's specific social climate.

In terms of course concepts, the paper connects directly to information security policy (ISP) compliance, organizational culture, trust in leadership, and human error. Rather than treating policy violations as individual moral failures, Ghaleb shows that organizational culture drives human error. Regarding marginalized groups, this study sheds light on the experiences of lower-level administrative and non-technical staff. These employees are frequently treated as workplace scapegoats and blamed for corporate data breaches, even though they are rarely given proper structural training or supportive environments.

Overall, the study makes two major contributions to society: it gives companies a practical blueprint to prevent expensive data breaches through better leadership rather than just expensive software, and it encourages healthier, trust-based workplace cultures over punitive monitoring.

2. Lins, Greulich, Pienta, Thatcher, & Sunyaev (2026)

Lins et al. investigate the psychological impact of cyber threats on workers, specifically introducing the concept of "security perplexity." The authors set out to answer how threatening and ambiguous cyber incidents induce mental strain in employees, and how this psychological state affects their real-time decision-making. To study this, the researchers used a mixed-methods design, combining multi-wave surveys with scenario-based behavioral experiments to observe subjects under simulated high-stress conditions. They analyzed the resulting data using quantitative inferential statistics, including Analysis of Variance (ANOVA) and regression analysis, to track cognitive load, confusion, and error rates.

This study embodies the social science principle of skepticism by actively challenging the lazy assumption that employees fall for security traps out of carelessness. Instead, it proves objectively that failures stem from cognitive overload. It also demonstrates objectivity by using standardized stress

metrics, and parsimony by distilling complex emotional reactions down to the single, powerful concept of security perplexity.

The findings tie directly into course concepts such as social engineering, phishing, cognitive strain/overload, and psychological vulnerability. The researchers prove that cybercriminals purposely design threats to cause panic and confusion, directly exploiting human cognitive limits. When looking at marginalized populations, this paper is especially relevant for neurodivergent employees and older, less tech-savvy workers. These individuals often experience heightened anxiety and digital stress when subjected to high-pressure, manipulative social engineering attacks, making strict, high-stress security drills counterproductive for them.

Societally, this paper provides immense value. It helps organizations build empathetic, realistic security training programs that reduce employee burnout, while simultaneously protecting critical public and business infrastructure by teaching people how to navigate high-pressure phishing and ransomware attempts without panicking.

3. Maringa & Nelson (2026)

Maringa and Nelson shift the focus to higher education, evaluating how institutional weaknesses create opportunities for cybercrime. Their qualitative case study focused on the University of Venda in South Africa, asking what specific institutional, policy, and human-factor vulnerabilities leave universities exposed to cyber threats. The researchers conducted structured focus group discussions with campus Information Communication Technology (ICT) officials and network administrators. They then used thematic analysis to analyze the qualitative transcripts, identifying common themes surrounding administrative oversights, weak policies, and poor user practices.

The study aligns with key social science principles, including empiricism, by gathering direct qualitative evidence from IT professionals on the ground. It also illustrates relativism by demonstrating that cybersecurity strategies must be evaluated relative to an institution's specific resources and

geographic context, alongside ethical neutrality, as the authors analyze system failures without unfairly vilifying the university staff.

The paper integrates seamlessly with class concepts like Routine Activity Theory, where the university serves as a "suitable target," cybercriminals act as "motivated offenders," and missing policies represent an "absence of a capable guardian." It also highlights issues surrounding password hygiene, incident reporting protocols, and overall institutional vulnerability. The study explicitly addresses marginalized groups by focusing on historically underfunded rural universities in the Global South and students from low-socioeconomic backgrounds. These groups face a severe digital divide, lacking access to early digital literacy and modern IT infrastructure, which leaves their sensitive personal data highly vulnerable to exploitation.

Ultimately, this study contributes to society by offering a practical framework for resource-constrained public institutions to protect their networks. By helping secure higher education systems, it protects sensitive student data and ensures equal access to uninterrupted education for disadvantaged communities.

4. Vharhe & Ateduobie (2026)

Vharhe and Ateduobie examine the socio-economic drivers behind youth involvement in cybercrime. Their study set out to determine what social, economic, and psychological factors motivate young people to engage in activities like online fraud, cyberbullying, and cyberstalking, and whether community-based social entrepreneurship can divert them from criminal behavior. The authors conducted a quantitative field survey of 317 youth participants across Edo State, Nigeria. They analyzed the data using descriptive statistics and inferential Chi-square tests to draw clear empirical connections between economic conditions and illegal cyber activities.

Social science principles are central to this paper. The study relies heavily on determinism, proving that youth cybercrime is primarily driven by systemic poverty, unemployment, and lack of

opportunity rather than inherent criminal intent. It also reflects relativism by highlighting regional economic dynamics, and objectivity by measuring crime through empirical survey data rather than sensationalized media narratives. The article connects directly to class topics such as motivations for cybercrime (like financial survival, revenge, and peer status), cyberbullying, cyberstalking, deterrence theory, and social entrepreneurship.

This research directly targets two marginalized groups: economically disenfranchised youth in developing nations, who turn to cybercrime due to systemic unemployment, and young victims of online harassment, who often lack legal protection or mental health resources. The societal contributions of this study are profound. It proves that tackling global cybercrime requires addressing root socio-economic causes like poverty and youth unemployment. Rather than relying solely on punitive legal action, the authors offer policymakers a roadmap for turning technical youth talent toward legitimate, community-building entrepreneurial ventures.

Conclusion

When evaluated together, these four studies reveal a clear social science consensus: technological defenses are only as reliable as the human systems surrounding them. While Ghaleb (2025) and Lins et al. (2026) emphasize the internal corporate environment, showing that policy compliance relies on trust, culture, and manageable stress levels, Maringa & Nelson (2026) and Vharhe & Atedubie (2026) expand the scope to broader institutional and regional contexts. They prove that resource deficits, poor policy, and economic hardship create the exact conditions that cybercriminals exploit.

Ultimately, applying social science principles to cybersecurity proves that keeping digital environments safe isn't just a matter of writing better code. It requires building healthy workplace cultures, reducing human stress, supporting underfunded public institutions, and providing economic opportunities for youth.

References:

Ghaleb, M. (2025). Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management. *International Journal of Cyber Criminology*, 19(1), 1–26.

<https://cybercrimejournal.com/menuscrypt/index.php/cybercrimejournal/article/view/437>

Lins, S., Greulich, M., Pienta, D. A., Thatcher, J. B., & Sunyaev, A. (2026). The impact of threatening cybersecurity situations on employees: A conceptualization of security perplexity. *Information Systems Research*. Advance online publication. <https://doi.org/10.1287/isre.2023.0626>

Maringa, M., & Mulaudzi, A. N. (2026). Evaluation of higher learning institutions cybersecurity in tackling cybercrime: A review of University of Venda Information Communication Technology officials. *International Journal of Research in Business and Social Science*, 15(1), 31–40.

<https://doi.org/10.20525/ijrbs.v15i1.4625>

Vharhe, O. H., & Ateduobie, W. (2026). Cybercrimes and cyber security among youth in social entrepreneurship venture approach. *International Journal of AI Ethics and Society*, 2(1), 1–25.

<https://journals.chroniva.org/index.php/IJAES/article/view/43>