

Annotated Bibliography

Nicholas Duggins

Matthew Umphlet

07/05/2026

Annotated Bibliography

Introduction

Cybersecurity is often viewed as a technological issue, but many successful cyberattacks occur because cybercriminals exploit human behavior rather than computer systems alone. People commit cybercrime for many reasons, including financial gain, revenge, curiosity, entertainment, and recognition. At the same time, organizations become vulnerable because of human error, poor security awareness, weak security policies, and ineffective organizational practices. The four scholarly articles in this annotated bibliography examine the social science aspects of cybersecurity by exploring employee behavior, organizational culture, psychological responses to cyber threats, and the human factors that influence cybercrime. Together, these sources provide a better understanding of how human behavior affects both cybercriminal activity and cybersecurity defenses.

Annotated Bibliography

Ghaleb, M. (2025, June). 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/menuscript/index.php/cybercrimejournal/article/view/437>

This peer-reviewed study examines how cybersecurity awareness, organizational culture, and trust in management influence employee compliance with information security policies. The researcher collected data from 261 employees working in different departments and used statistical analysis to evaluate the relationship between these factors. The findings revealed that organizations with strong cybersecurity awareness programs and positive workplace cultures are more likely to have employees who follow security policies and engage in secure behaviors. The study also found that trust in management plays an important role in encouraging employees to comply with cybersecurity requirements.

This article is valuable because it focuses on the human side of cybersecurity rather than the technical side. Many cyberattacks are successful because employees make mistakes or fail to follow security procedures. The study demonstrates that creating a culture of security and trust can reduce these vulnerabilities. This source is highly relevant to my topic because it shows how human behavior within organizations can either strengthen or weaken cybersecurity defenses. It also provides practical solutions for reducing the opportunities that cybercriminals exploit.

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://pubsonline.informs.org/doi/full/10.1287/isre.2023.0626>

This article introduces the concept of “security perplexity,” which refers to the confusion, uncertainty, and stress employees experience when faced with sophisticated cyber threats. The researchers analyzed hundreds of survey responses and experimental results to better understand how individuals react when confronted with complex cybersecurity situations. Their findings suggest that employees often experience high levels of cognitive stress when they are unsure how to respond to potential cyber threats. Depending on the situation, this stress can lead to either effective decision-making or actions that increase security risks.

This source is important because it explains how cybercriminals take advantage of human psychology. Many phishing attacks, ransomware campaigns, and social engineering schemes are designed to create urgency and confusion. By understanding how employees respond under pressure, organizations can develop training programs that help reduce mistakes during cybersecurity incidents. This article supports my research by showing that human decision-making is often one of the most vulnerable points in an organization's cybersecurity strategy.

Maringa, M., & Nelson, A. (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 & Social Science*, 15(1), 31–40.

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

This qualitative case study investigates cybersecurity practices within a higher education institution in South Africa. The researchers conducted focus group discussions with information technology officials to identify cybersecurity challenges facing the university. Their findings revealed several weaknesses, including a lack of cybersecurity policies directed toward students, poor awareness of incident reporting procedures, and inadequate password management practices. These weaknesses created opportunities for cybercriminals to target the institution and exploit preventable vulnerabilities.

I found this article useful because it applies social science and criminological concepts to a real-world setting. The study shows how poor security awareness and weak institutional policies can create opportunities for cybercrime. This source is relevant to my topic because it demonstrates that cybersecurity is not only about technology but also about education, communication, and individual responsibility. The findings highlight how simple human errors and organizational failures can increase the likelihood of cyberattacks.

Vharhe, H. O., & Ateduobie, W. (2026, January 29). *Cybercrimes and cyber security among youth in social entrepreneurship venture approach. International Journal of AI Ethics and Society*, 4(2), 45–60. <https://journals.chroniva.org/index.php/IJAES/article/view/43>

This study explores cybercrime and cybersecurity issues among youth populations in Edo State, Nigeria. Using survey data from 317 participants, the researchers examined common forms of cybercrime, including cyberbullying, cyberstalking, and online financial fraud. The results showed that these activities negatively affect cybersecurity efforts and create challenges for local communities and

organizations. The authors recommend increased cybersecurity education, awareness programs, and community-based interventions to help reduce cybercrime among young people.

This article is particularly relevant because it examines the motivations behind cybercrime among younger populations. Financial fraud highlights the role of economic incentives, while cyberbullying and cyberstalking often involve personal conflicts, revenge, or misuse of technology. The study supports the idea that cybercrime is driven by a variety of social and behavioral factors rather than purely technical ones. This source strengthens my research by providing real-world examples of how human motivations influence cybercriminal behavior and contribute to cybersecurity challenges.