Dylan Shaver

Professor Yalpi

CYSE 201S

April 13, 2025

The Role of Social Science in the Career of a Cybersecurity Analyst

BLUF: While technical expertise forms the foundation of a cybersecurity analyst's responsibilities, integrating social science principles provides a more complete approach to protecting digital systems. A firm grasp of human behavior, organizational environments, and societal influences enhances an analyst's ability to design effective, inclusive, and adaptive security strategies. Additionally, knowledge of cybercrime, cybercriminology, and cyber law equips analysts with tools to navigate today's complex threat landscape

Understanding Human Behavior in Cybersecurity: Many cyber incidents stem from human mistakes, clicking on phishing emails, using weak passwords, or unknowingly exposing confidential information. Fields like psychology and sociology provide valuable insights into why users behave the way they do. Herath and Rao (2019) argue that recognizing decision-making patterns is crucial to improving information security. When analysts understand these patterns, they can tailor training programs that change behavior, simplify procedures to avoid confusion, and identify where user habits might create risks. Zabeb (2024) adds that social science makes it possible to design user-friendly and ethical policies that maintain protection without alienating users. In a similar vein, cyber criminology helps analysts understand criminal intent and behavior, allowing them to proactively identify risks such as identity theft and hacking before these threats become full-blown attacks (Carley et al., 2020).

Organizational Culture and Security Effectiveness: Security doesn’t exist in a vacuum; it’s shaped by the workplace environment. According to Carley et al. (2020), cybersecurity is as much a social challenge as it is a technical one. An organization’s internal dynamics, communication structures, and openness to innovation all influence how well it adopts cybersecurity protocols. For example, an organization that encourages cross-team collaboration and prioritizes education may detect and report threats more effectively than one with a rigid hierarchy and poor information flow.

Bhuit (2024) highlights that security policies aligned with an organization’s unique social framework are more likely to be accepted and followed. Analysts who understand this can craft policies that respect workplace norms while still upholding digital safety. Moreover, cyber law plays a critical part in ensuring policies align with legal requirements. Regulations on data protection, intellectual property, and digital privacy shape how organizations build and implement cybersecurity defenses. Analysts benefit from social science research when interpreting how different institutions and societies enforce these laws (Zabeb, 2024).

Societal Inequities and Cybersecurity Vulnerabilities: The internet reflects real-world inequalities. Vulnerable and underrepresented groups often face greater risks online. Bada and Nurse (2019) explain that cyber attackers frequently exploit these social vulnerabilities. Analysts who apply social science can better understand the specific conditions that put certain communities at higher risk. By acknowledging the social, economic, and psychological circumstances that increase susceptibility to online crimes, analysts can create more equitable and targeted solutions.

Cyber criminology also plays a role in identifying trends and motives behind online crime. Analysts who understand how criminals exploit cultural and societal weaknesses can partner with law enforcement to build more effective prevention strategies. Bada and Nurse (2019) note that this type of collaboration can be especially powerful when defending high-risk communities.

Furthermore, the call for more diverse representation in the cybersecurity field is essential. Teams that reflect a wide range of backgrounds are more likely to notice overlooked vulnerabilities and propose well-rounded solutions (The World Economic Forum, 2021).

The Push for an Inclusive Cybersecurity Workforce: Building a diverse cybersecurity community isn't just about fairness, it directly impacts performance and innovation. Herath and Rao (2019) argue that inclusive workspaces foster collaboration and attract talent that might otherwise be overlooked. Programs like TransTech, which offer job training for LGBTQ+ professionals, show how intentional support can lead to real progress (Zabeb, 2024).

Social science tools also help analysts identify hidden barriers to diversity and inclusion. Once these roadblocks are known, organizations can take steps to remove them—whether through mentorship programs, policy changes, or updated hiring practices. Diverse teams bring multiple perspectives, which is especially important when building strategies that must work for many different types of users (The World Economic Forum, 2021).

Conclusion: Cybersecurity today requires more than technical knowledge, it demands a well-rounded understanding of people, cultures, and the social systems they operate in. When cybersecurity analysts apply social science insights, they improve their ability to predict user behavior, respond to threats with empathy and fairness, and develop policies that both protect and include. Fields like cybercriminology, cybercrime analysis, and cyber law provide a legal and behavioral framework that complements technical defenses. In the end, blending technical skills with social science insight is the key to building a safer, more inclusive digital future.

References

Bada, M., & Nurse, J. R. C. (2019). The social and psychological impact of cyber-attacks: A review and future agenda. *Computers & Security, 87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Bhuit, T. (2024, April 8). *The role of social science in cybersecurity policy analysis*. Old Dominion University. https://student.wp.odu.edu/bhuit001/2024/04/08/the-role-of-social-science-in-cybersecurity-policy-analysis/

Carley, K. M., Malik, M., Landwehr, P. M., Pfeffer, J., & Kowalchuck, M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory, 26*(4), 365–375. https://doi.org/10.1007/s10588-020-09322-9

Herath, T., & Rao, H. R. (2019). Social science in information security research: An interdisciplinary approach. *Information & Management, 56*(2), 225–235. https://doi.org/10.1016/j.im.2018.06.004

The World Economic Forum. (2021, October 7). *Why cybersecurity needs a more diverse and inclusive workforce*. https://www.weforum.org/stories/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/

Zabeb, B. (2024, April 23). *The role of social science in the work of cybersecurity analysts*. Old Dominion University