Cybersecurity Analysts

Emmanuel Walker

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

11/16/2025

The field of cybersecurity is a broad range of professions that involve both technological expertise and a thorough understanding of human behavior. One occupation that stood out to me is cybersecurity analysts, whose primary responsibility is to defend businesses from cyber threats while tracking networks and taking measures to prevent them. While technical skills such as malware analysis, firewall configuration, and coding are all important, professionals in the IT field also rely extensively on social science research and principles. Understanding human behavior and critical thinking is essential for responding to cybercrime.

To minimize the risks, cybersecurity analysts apply concepts from behavioral science, criminology, and organizational sociology in their work. “Cybersecurity behavior is essential to protecting organizations and individuals from security threats” (Almansoori et al., 2023). For example, Behavioral Theory explains how employees' behaviors and decisions might contribute to weaknesses like clicking on phishing links or giving away sensitive information.
Professional analysts conduct training programs that favor safe behaviors, so directing business culture toward security protocol compliance will better everyone's safety in cyber space. Also, Routine Activity Theory principles help analysts in identifying possible targets and "to understand the factors influencing cybercrime victimization" (Ahmad & Thurasamy, 2022) in network security. Analysts use human behavior patterns and social circumstances to predict attack routes and insider dangers. This article underlines the principles of this theory and how it aligns well with this job I wish to pursue.

Cybersecurity analysts use ideas from social sciences in their daily operations. They send out warnings to different people that may be in a situation where they may be doing something they shouldn't be doing while keeping in mind human nature that could interfere with what is happening. Humans make mistakes in solving situations, so other analysts from the team will help in the need because they are the backbone of cyber protection. For example, if a user consistently violates security procedures, analysts may detect a training deficit or a behavioral problem inside the organization, which they can address by education or making policy changes. "Professionals must consider the social consequences of their actions, decisions often grounded in ethics, public policy, and human rights principles" (*The Social Science)*. When communicating risks to stakeholders, analysts also use psychological and sociological knowledge to ensure that messages are understood by a wide range audiences and produce behavioral change. These applications help the analysts understand their role and for them to exceed that role.

Their skills also analyze how their work affects marginalized groups. Migrant workers and low-income populations are more vulnerable to cybercrime due to a lack of digital knowledge or access to secure technology. Analysts must create accessible awareness programs to ensure the protection of all employees or users, regardless of socioeconomic level. Analysts do not only contribute to the people of society, but also to different areas around the world protecting financial systems. All these different companies have valuable items attached to it like passwords to electronic systems or money transfers. Hackers are going to attack what is easiest to them, therefore having the people of the company make strong password protection, cybersecurity analysts are the second step into preventing these attacks.

In conclusion, cybersecurity analysts play a key role at the center of technology, human behavior, and society. Analysts use social scientific ideas to not only prevent and respond to cybercrime, but also to change business culture and ensure equal protection for minority groups. Their study shows the critical role of social science knowledge in technical cybersecurity jobs knowing that both technological and human components are to provide successful digital security. As cyber risks continue to expand throughout the years, social science-informed cybersecurity analysis becomes more important for businesses and society as a whole.

Ahmad, R., & Thurasamy, R. (2022). A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes. *Journal of Cyber Security and Mobility*, *11*(3). https://doi.org/10.13052/jcsm2245-1439.1133

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Sciences*, *13*(9), 5700. https://doi.org/10.3390/app13095700

The Social Science Behind Cybersecurity Analysts' Work | tiyaralavon. (2025, April 30). Odu.edu. https://sites.wp.odu.edu/tiyaralavonfitz/2025/04/30/the-social-science-behind-cybersecurity-analysts-work/