Caitlene Baer **11/16/2025**

Cybercrime Analysts: The Social Science Foundations of a Cybersecurity Career

Introduction

The field of cybersecurity has become one of the most crucial professions in the digital age. With technology becoming so important in financial networks, healthcare networks, schools and state entities, the level of threat surrounding cybercrime is growing substantially. Cybercrime analysts, who specialize in investigating offenses committed through technology, find patterns of criminal behavior, and help law enforcement agencies, work diligently to protect society from cyber crime. This paper illustrates the ways that cybercrime analyst as a profession is influenced by social science research and how their daily work is influenced both positively and negatively by human behavior, criminology, and sociology. It also discusses how cybercrime changes marginalized populations, who cybercrime analysts interact with outside of the profession and what social science research provides about the social worlds of these professionals.

Social Science Principles in the Cybercrime Analyst Career

Cybercrime analysts use social science research because fundamentally, cybercrime is a human action manifested through digital means. (Holt & Bossler, 2021). Explaining why offenders engage in hacking, fraud, harassment, or identity theft requires the same principles that criminology uses—motivation, opportunity, and social pressure for encouraging criminal activity. Social science allows analysts to know about offender profiling, patterns of behavior, and sociological factors that produce deviant behavior online. (Ghaleb, 2024).

These principles also guide practical cybersecurity activities. For example, analysts use human-computer interaction research and its findings to understand how users accidentally expose a system to risk, such as falling victim to phishing. The work psychology has carried out about cognitive biases informs analysts about the places for vulnerabilities to appear. Social science thinking also helps cybersecurity practitioners in developing their awareness training program by outlining how humans learn and alter behavior as a response to issues of authority. (Ghaleb, 2024). By understanding how humans decide, cybercrime analysts can develop and design a better educational method and construct more persuasive messages about security purposes that can be used to decrease risk within an organization.

Application of Key Concepts

Several core ideas from cybersecurity and social science classes are relevant to the role of a cybercrime analyst. Many terms like routine activity theory, the victim-offender overlap, and social engineering come in play, often multiple times in investigations. (Holt & Bossler, 2021). For instance, routine activity theory is used to predict the time of day or week when a computer or an individual may be at their most vulnerable based upon online habits and patterns of digital behavior. A professional understands the victim-offender overlap, and how an individual may perpetrate an offense, while simultaneously being victimized, which is common in cyberspace (cyberbullying and online harassment).

Cybercrime analysts also often apply theories of organizational behavior to assess internal vulnerabilities, develop a strategy for a potential insider threat, or ensure policy practice compliance with federal regulations such as HIPAA, or "The Computer Fraud and Abuse Act." Utilizing tools such as digital forensic software, profiling strategies, and behavioral analysis, cybercrime analysts act as detectives piecing together evidence from the digital world while also trying to assess motivations and methods behind a cyberattack. In this way, a cybercrime analyst's work integrates technical capability in the cyber environment with sociological and psychological frameworks for investigating the related human behavior. (Leukfeldt & Yar, 2016).

Marginalization in Cybersecurity and Cybercrime

Cybercrime affects marginalized groups—people who identifying as low-income, elderly, racial minorities, limited experience using technology, and unequal access to cybersecurity education and resources (such as institutions)—more often and more severely. (Holt & Bossler, 2021). The impact is endured by these groups who are more prone to the unequal distribution of cybersecurity knowledge, resources, and institutional favor. Cybercrime analysts must understand this context as they conduct investigations, start interventions, and/or engage in preventive measures. Knowledge about the disproportionate impact of cybercrimes on marginalized groups has been documented in the research literature related to marginalized communities being more often the target of frauds, identity theft, and harassment among others, which contributes to social inequality.

As a reaction, the field of cybersecurity has started to promote awareness and education on digital inclusion, build more security awareness programs, and increase the diversity within the field. Cybercrime analysts contribute to this by finding patterns of cyber victimization that disproportionately change vulnerable populations seeks change in policies that would build protections for marginalized groups vulnerable to cybercrimes. Thus, fair digital safety is an emerging ethical responsibility for those in the cybersecurity field.

Career Connection to Society

Analysts specializing in cybersecurity support societal safety and security through their efforts to safeguard critical infrastructure in cyberspace. They also serve a supportive role in investigations and prosecutions started by law enforcement and contribute to national security efforts, in addition to ensuring that cyber criminals have not launched attacks against hospitals, schools, banks, and government agencies. (Leukfeldt & Yar, 2016). Their work often involves creating analysis reports that underpin public policy design, often in drafting new statutes that will address new and evolving risks for constituents.

Statutes in cybersecurity such as data breach notification laws, and privacy laws, as well as laws addressing cyber crime would not be possible without cyber crime analysts specializing in the analysis of criminal behavior in cyberspace. (Holt & Bossler, 2021). As cyber threats become more aggressive, the work of cyber crime analysts will become even more valuable in improving societal resilience, as well as restoring and supporting public faith in digital systems.

Conclusion

Cybercrime analysts rely on principles of social sciences to balance the human-centric nature of digital crimes. Concepts of psychology, sociology, criminology, and organizational behavior applied to the analysis of digital crimes, prediction of offender behavior, and improvement of safety on the internet. The work cybercrime analysts do benefits society at each level—from protecting critical infrastructures, helping law enforcement, and supporting equity amongst marginalized groups. As cyberattacks evolve, the union of social science and cybersecurity skills found in cybercrime analysts is a valuable resource for protecting safety, justice, and trust in the online world.

References

Ghaleb, M. M. S. (2025). Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture, and trust in management. International Journal of Cyber Criminology https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123

Holt, T. J., & Bossler, A. M. (2021). *Cybercrime and digital criminology*. Routledge. https://www.routledge.com/Cybercrime-and-Digital-Forensics-An-Introduction/Holt-Bossler-Seigfried-Spellar/p/book/9780367360078

Leukfeldt, R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. https://www.tandfonline.com/doi/full/10.1080/01639625.2015.1012409