Cybercrime Investigators

Richard W. Young

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Matthew Umphlet

April 9th, 2024

Cybercrime Investigators

Cybercrime investigators play a key role in identifying, apprehending, and prosecuting cyber criminals. They also have the tools and knowledge required for hardware or software penetration testing, damaged file system recovery, and cyber threat incident response. The label cybercrime investigator can be broad, but the type of work they execute actively and proactively helps secure critical data and bridges gaps between private and public sectors.

Investigators can apply different research methods and social sciences to further their investigations. Investigators need to understand that the social sciences adhere to the same concepts as natural sciences. To explain further, a few social sciences that can be applied to cybercrime investigations are relativism, objectivity, parsimony, skepticism, ethical neutrality, and determinism. Psychological theories and principles can be used to understand the motives and behaviors of cybercriminals, which would aid in the possible intervention or prediction of future cybercrime. Sociological analysis, like economic conditions, peer influences, and cultural norms, can help investigators understand broader contexts of certain cybercrimes. An example of a psychological theory that can be applied to how investigators use social sciences could be victim precipitation. This theory implies that victims are classified as easy or hard targets before the crime occurs.

Cybercrime investigators are tightly interconnected with society. With the growth of interconnectedness through the internet and technology, many people rely on using the internet everyday for different purposes. When the world is connected through the internet in so many different ways, bad actors have a variety of opportunities to use technology against others. Deora et al (2021) listed the most common cybercrimes as cyberbullying and harassment, financial

extortion, internet threats, global security data theft, password trafficking, personal data hacking, copyright violation, illegal weapon trafficking, child pornography, credit card theft and fraud, email phishing, cyber espionage, and virus spreading. For a cybercrime investigator to collect evidence used against criminals, he or she must be well-connected with the popular applications that the public is using. They must also find strategic ways of navigating through maintaining the privacy of anyone involved in the cybercrime and navigating through collaboration with law enforcement, researchers, and government regulators. This can be challenging because Al-Khater et al (2020) explains that the data needed for prosecution or cybercrime profiling is "mostly critical, sensitive, and private."

Broken down to the lowest level, the two main parties involved in cybercrime are the victim and the criminal. Cybercrime investigators need to understand which marginalized groups are targeted the most. Sviatun et al (2021) mention that "the most vulnerable areas are those that use electronic computing and the internet in their work as well have a large financial turnover: financial, retail, communication, and technology." A few challenges that arise when cybercrime investigators investigate different crimes would be a lack of accurate data, privacy laws, and politics. Researchers and cybercrime investigators need to study cybercrime at every scale, apply social science principles, and apply different research techniques to actively and proactively secure networks that store critical data with how connected civilization is becoming with technology and the internet.

References

Al-Khater W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*. *8*, 137293-137311. 10.1109/ACCESS.2020.3011259

Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6. 10.37591/JoCES

Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762. 10.37394/23207.2021.18.72