

Career Paper

Zoe Koch

CYSE 201S

Cybersecurity is an expansive field with plenty of career paths to follow. It's a field that continues to grow more prominent day by day due to the popularity and significance of technology and information technology. Cybersecurity has been an interest of mine from a young age, and thanks to Old Dominion University introducing me to criminology, it has led to my growing interest in cybercrime investigation. Cybercrime investigators are "primarily concerned with gathering evidence from digital systems that can be used in the prosecution of internet-based, or cyberspace, criminal activity" (Bowcut, 2022). As such, they are often directly involved or in line with social sciences.

Cybercrime investigators have a direct relationship with society due to their obligations to protect. For instance, it's estimated that 40% of the world's population has access to technology and 5 billion people across the world own some sort of mobile device (Darina, 2022). As a result, people are beginning to feel more comfortable with technological use and are finding ways to abuse it. These cyber-threats can financially, emotionally, and physically harm the people they assault. Society relies on cybercrime investigators to protect and secure their data, and to act when laws are broken or when people are at risk. Much like how police officers or criminal investigators work with society to take down criminals, cybercrime investigators have a similar symbiotic relationship with society. Cybercrime has reached a point where it's no longer considering just technical solutions, but also human solutions (Amos et al., 2021).

The social science principles offer a great perspective on how cybercrime investigators react to opportunities and situations. The social science principles are a set of values that cybercrime investigators (and criminal investigators) can rely on when conducting investigations. Determinism offers a pattern to follow, relativism offers an idea of consequence and reaction to the situation, and skepticism allows them to keep their mind open. Cybercrime investigators must also utilize objectivity and ethical neutrality to ensure that what they're doing is ethical and within principle, additionally, they can utilize parsimony to make it easier for society and criminals to understand what was wrong. In terms of social science research, cybercrime investigators can use the patterns and deeper information about criminal activity to get a better understanding of potential attacks and opportunities to prevent data from being compromised.

Outside of the social science principles, there are a handful of additional concepts that cybercrime investigators should consider when doing their job or following their career path. The first concept that cybercrime investigators need to consider is victimization. Amos et al. (2021) found in recent surveys that 60-90% of cyber incidents are caused by human error. Whether that be clicking a suspicious link, falling for a phishing scam, or accessing sites that should not be accessed – cybercrime investigators need to consider victim precipitation or the role the victim plays in the victim experience. Victims are never at fault for the crimes committed against them, but by having a deeper understanding of the role they play, cybercrime investigators can get a better idea of how the crime was committed and who was behind it.

This is where human factors play an additional role, another key concept. Human factors, or how human intervention plays a role in cybersecurity. Cybercrime investigators are one of many human factors, their actions in cyber space make a difference. Human factors can allow cybercrime investigators to reduce human error and improve security.

By getting an idea of how a victim is placed within the crime scene, a cybercrime investigator can begin to understand the motive. Motive is another concept that can be applied to cybercrime investigators because by understanding the motive, whether it's financial, personal, or out of boredom, a cybercrime investigator can begin to pin together the perpetrator behind the crime. Additionally, it helps form a pattern of if the criminal will recommit the crime or the target victims they're after.

Cybercrime investigators do what they do to protect the people but to also exercise cyberlaw (another crucial concept). Cyberlaw is broad and can be hard to define because of how new technology and cybercrime are as a whole, not many laws have been made to cover cyberspace. Most laws are vague or offer a lot of gray areas, which cyber criminals exploit. Cybercrime can include the violation of intellectual property, computer abuse with intent, computer crimes that violate specific laws, and computer-related crimes. Additionally, cybercrime investigators are also susceptible to breaking the law. They must have a good understanding of the laws and cyber laws in their area so that they investigate within their legal boundaries.

In terms of the cybersecurity field, marginalized groups can include women, children, people of color, and communities and ethnicities that are discriminated against. The discrimination that

occurs within the physical space is also very real in cyberspace. Many marginalized groups face discrimination because of how they look, where they are from, or because they are (or were) previously seen as lesser than a white male. Cyberbullying amongst children on social media is a common challenge that arises because it's easy, and most times nothing is done about it. Children of color or marginalized groups are more at risk for cyberbullying and often more in danger because there is little they can do about it. Thankfully, cybercrime investigators and other organizations are advocating for the awareness of cyberbullying (which will eventually lead to cyberbullies receiving punishment for their crimes). Additionally, marginalized groups are more vulnerable to these crimes because of the belief that they are lesser. Some cyber criminals will only attack marginalized groups, in which cybercrime investigators are not only seeing cybercrimes but also hate crimes. Another issue that arises amongst marginalized groups and cybercrime investigators is that the field is dominated by white males. Marginalized groups have a more difficult time getting introduced to the field because they may not receive the right aid or feel discouraged because of a lack of similar people in the field.

References

- Amos, Z., Coguic, D. L., Biseul, X., Pommeraud, J., Deblock, F., Joos, T., Dalleau, R., Coillet-Matillon, P., Auberger, C., Auxenfants, M., Benzaquen, M., Beyrouthy, A., Hearn, P. W., Stamboliyska, R., Raffray, M., Przyluski, V., & Dreidemy, P. (2021, September 2). *Social Science and cybersecurity: A key challenge for the future*. InCyber. Retrieved December 1, 2022, from <https://incyber.org/en/social-science-and-cybersecurity-a-key-challenge-for-the-future/>
- Anonymous. (n.d.). *Cyber crime investigator - NICCS*. Retrieved December 1, 2022, from https://niccs.cisa.gov/sites/default/files/documents/pdf/cyber-crime-investigator_508c.pdf?trackDocs=cyber-crime-investigator_508c.pdf
- Bowcut, S. (2022, April 21). *How to become a cybercrime investigator: A complete career guide*. Cybersecurity Guide. Retrieved December 1, 2022, from <https://cybersecurityguide.org/careers/cyber-crime-investigator/>
- L., Darina. "How Fast Is Technology Growing Statistics [Updated 2022]." *Best Tech Jobs Near You*, Leftronic, 26 Apr. 2022, <https://leftronic.com/blog/how-fast-is-technology-growing-statistics/>.