

Career Professional Paper

With every passing year, we see exponential growth in technology as well as a growth in internet technology. Advances in these two, especially internet technology, bring both beneficial and harmful impacts to society. IT has become so advanced that merely everything is connected to it. Unfortunately, we are tending to see that people are using this advancement for harm rather than its intended purpose. To defend such acts we have set aside human factors as well as technical safeguards. We have coined this protection with the term Cybersecurity. Though, with Cybersecurity being relatively new, I have noticed that there is a stigma that has formed that Cybersecurity is only a technical-based profession and specialty. This proves to be incorrect. Like most tech professions, Cybersecurity is interdisciplinary. Coexisting with the Social sciences, Math, Technology, Science, Engineering, etc. For this paper, I am going to be focusing on the relationship between Cybersecurity and the Social sciences. The Social sciences change the way we think, interact, and study Cybersecurity.

First and foremost, I want to discuss how the Social sciences affect the way we think of Cybersecurity and specifically cybercrime(what cybersecurity defends against). Like traditional or standard crime, when dealing with crime online we have to think of the social aspects that play into the criminals as well as their victims. For cyber offenders, it is important to find some of the motives and preexisting social behaviors to get an understanding of cybercriminals. Venelin Georgiev, a professor at New Bulgarian University, discusses the use of identifying human roles in cybercrime. Just like “traditional” crime investigators, cybercrime investigators use profiling to assist in identifying cybercriminals(1). Profiling criminals is to look at the psychological behavior, race, gender, personality traits, etc of cybercriminals to, as I stated

earlier, assist investigators in detecting the criminals(2). Georgiev describes cybercriminals to have “minimal technical knowledge and skills”, “disrespect for the law”, “high-risk appetite”, and “strong, albeit... radical motivation”(1). As well as these characteristics, cybercriminals’ motives vary from political influence, sexual behavior, monetary gain, entertainment value, etc(1). When creating these profiles we are able to find patterns of these characteristics amongst cybercriminals. These patterns are crucial to help understand and defend cybercriminals. It goes to show how cybersecurity goes deeper than just the technical safeguards. While implementing technical defenses is important, identifying the “why” of the attack is just as necessary.

Though understanding cybercriminals, as well as their victims, is crucial to cybersecurity, another big factor that comes in is how we obtain the information. With this, I mean the research and study that is based around cybersecurity. There are multiple ways that research is conducted in cyberspace. These include but are not limited to observational research, theoretical research, experimental research, as well as applied research(3). These types of research are the foundation of most cybersecurity studies. From a social science point of view, cybersecurity researchers are bound to numerous principles when researching and creating cybersecurity studies. These principles include relativism, objectivity, parsimony, objectivity, parsimony, skepticism, ethical neutrality, and determinism(4). For example when conducting research about cybersecurity; researchers need to stay as objective as possible. In layman's terms, this means staying as fact-based as possible and excluding any opinionated or feeling-based statements. Following the principle of objectivity, researchers are able to keep their research and studies as neutral/fact-based as possible. When discussing the topic of possible punishments for cybercriminals, this principle is crucial to keep punishments as ethical as possible. While some may have passionate emotions about how to go out punishing cyber criminals, it's best to keep

research as unbiased as possible to 1. Get the most accurate outcome and 2. Keep things ethical(4)l. Though I only described one of these principles, cybersecurity researchers and professionals are held to the standard of all seven of these social science principles.

In conclusion, cybersecurity is an interdisciplinary based profession. When conducting any work in the field, neglecting even one of the disciplines may result in possible flaws in the work. From research to defending from hackers, every aspect, either social or technical, is crucial to take into account. This is why cybersecurity professionals are pushed to constantly learn all disciplines of the field to be as equipped as possible when pursuing any form of cybersecurity profession. The stigma I discussed previously must be diminished for the best interest of cyberspace security. I, myself, once had this same stigma. Learning about the broad horizon of cyber has pushed me to better understand cybersecurity as a profession. While being able to branch out and master one subgroup of cyber is possible, it goes to show that knowing at least some of the other disciplines is important.

References

1. Georgiev, V. (2019). Profiling human roles in Cybercrime. *Information & Security: An International Journal*, 43(2), 145–160. <https://doi.org/10.11610/isij.4313>
2. Winerman, L. (2004). *Psychological sleuths--criminal profiling: The reality behind the myth*. Monitor on Psychology. Retrieved November 30, 2021, from <https://www.apa.org/monitor/julaug04/criminal>.
3. Edgar, T. W. (2017). Chapter 3. In D. O. Manz (Ed.), *Research Methods For Cyber Security* (pp. 63–74). essay, Elsevier. Retrieved November 28, 2021, from <https://ebookcentral.proquest.com/lib/odu/detail.action?docID=4848075>.
4. Payne, B. K. (2021, September). *Cyse 201S Module 2. Lecture*. Norfolk; Old Dominion University.