Alexander Turnsek

4/10/2024

Career Paper: Cybersecurity Analyst

Introduction:

In the field of cybersecurity, almost every job available depends on social science. A majority of cybersecurity work involves people and how they affect systems and data. This career paper will focus on the career of a cybersecurity analyst and how it depends on social science research and principles.

Relation to social science principles:

Cybersecurity requires social science to function, as people greatly influence the field. Social science principles allow cybersecurity analysts to find the causes of security breaches, such as the social science principle of relativism. Relativism refers to how a change can have a more significant effect on something, causing other things to change, like a system. Another good example is determinism, as analysts use it to figure out how a system was compromised and what led up to its breach.

Relation to Marginalized groups:

Cybersecurity analysts are closely related to marginalized groups, as each group has different cultures and rules regarding the use of technology. Some groups refrain from using technology often, which may make them more vulnerable as they have less experience with systems. Marginalized groups are also frequently targeted by malicious individuals.

Cybersecurity analysts must take precautions as some security issues do arise from marginalized groups' privacy. Gayle and Yuan said this when referring to the tech divide in marginalized groups: "...individuals excluded or increasingly disadvantaged are often the same marginalized populations most at risk during disasters" (Gayle & Yuan, 2024, p. 10)

Correlation to class concepts:

Being a cybersecurity analyst involves a lot of social science concepts like the Human-centered cybersecurity model, which says that humans are the center of a secure system. "Perhaps the greatest cybersecurity danger of all — whether for an individual, business, or government entity — is the possibility of human error" (Steinberg, 2022, p. 6). Another excellent example of concepts that fit with cybersecurity analysts is symbolic interactionism, which states that individuals understand society through interactions. Finally, the last two concepts that relate to cybersecurity analysts would be human factors and peer networking. These two relate to cybersecurity analysts by showcasing how human interactions affect the realm of cybersecurity.

Connection to society:

Cybersecurity analysts have a deep connection to society, as society shapes how cybersecurity analysts analyze systems. People are one of the most significant factors in cybersecurity. "It is difficult to overstate the importance of computer networks and cybersecurity in today's world." (Wu & Irwin, 2016, p. 2). From personal use to critical infrastructure, we actively rely on technology in various aspects of our daily lives.

Conclusion:

In conclusion, cybersecurity analysts' careers require social science principles and concepts. These concepts affect everything in cybersecurity, from how systems function to marginalized groups. Overall, Cybersecurity analysts need social science to function, and with it, they can figure out how people affect systems.

Reference List:

Wu & Irwin, J. D. (2016). *Introduction to Computer Networks and Cybersecurity* (1st ed.). CRC Press. https://doi.org/10.1201/9781466572140

Steinberg, J. (2022). *Cybersecurity for dummies* (2nd ed.). For Dummies. https://learning.oreilly.com/library/view/cybersecurity-for-dummies/9781119867180/?sso_link=yes&sso_link_from=old-dominion-university

Bennett Gayle, & Yuan, X. (2024). *Empowered or Left Behind: Use of Technology During COVID-19* (First edition, Vol. 1). CRC Press. https://doi.org/10.1201/9781003319894