Jacob Rivera
April 4, 2024

Cybersecurity Analysts and their Relation to Social Science

Overview:

There are many types of careers that revolve around the cybersecurity field. Cybersecurity analysts is what we will be examining in this paper. These experts could be compared to digital detectives. They are known to protect our online activities from cyber threats and hackers by investigating potential threats and implementing security policies. Although technical skills are very important to have, cybersecurity analysts also depend on social science research and principles. This paper will concentrate on how cybersecurity analysts work efficiently while applying social science concepts at the same time.

Importance of social science research and principles:

According to the CYSE201 module one powerpoint, social science can be referred to as "a group of scientific disciplines that study social phenomenon". Social science disciplines that are considered tenets of cybersecurity include psychology, political science, economics, criminology, and sociology. All of which cybersecurity analysts apply to their occupational lives. One discipline that I will be focusing on in this paper is psychology. Psychology is the study of the human brain and the way it behaves. In the context of cybersecurity, it helps us understand why people do what they do online, such as hackers and cybersecurity analysts who try to prevent them. Based on a study by The Sustainable Society Network, Their social psychology research focuses on "how the bahavior and cognition of individuals is influenced by the real, imagined or implied presence of others" (McAlaney 2016). By understanding the social perspective of cyber attacks, cybersecurity analysts can come up with better ways to stop them. This is similar to the concept "Psyber Security" that is mentioned in CYSE 201 module 4. The

article also shows how analysts that utilize psychology can make the digital world safer for everyone.

Cybersecurity Analysts and more Social Science Concepts:

Ethics is an important social science principle that cybersecurity analysts need to take into consideration while working. Ethics is about doing the proper thing, even when presented with tough situations. It is important because it influences their choices in an environment where their decisions can have huge consequences. This connects with a principle of science that is referred to in module 2: ethical neutrality. Regarding cybersecurity analysts, they deal with sensitive information and are tasked to create security measures that will protect people, the company, and society. Without ethics, analysts could take shortcuts in their work or prioritize personal interest rather than trying to benefit society. Kevin Macnish, a professor in the University of Twente, suggests that teaching ethics in computer science courses and making codes of conducts is a way for future cyber professionals to instill ethical guidelines. By following ethical guidelines, analysts can build thir trust and integrity (Macnish 2020).

Social cybersecurity is a fairly new scientific and engineering field. It is described to use "computational social science techniques to identify, counter, and measure the impact of communication objectives" (Carley 2020). It is basically about understanding how people behave online and how that will affect security. In a scholarly article that was featured in CYSE201 module 10, The author, Kathleen Carley from Carnegie Mellon University, writes a portion on how cybercriminals use social tactics to manipulate groups of people. As a cybersecurity analyst, you need to know how these harmful tactics are formed and used against society. With the understanding of social cybersecurity, you can protect against these tactics and keep people online safe.

Conclusion:

While the use of technical skills are needed for cybersecurity analysts, they also rely on social science research and principles to do their job efficiently. Throughout this paper, the scientific discipline of psychology allows analysts to understand why people make certain decisions and how to make policies around it. The social science principle of ethics helps analysts create efficient strategies against cyber threats with integrity. With the rise of social cybersecurity as a new field, it is important for analysts to understand the concept as it will allow them to stay ahead of emerging threats and, overall, digitally protect society.

Referenecs:

Carley, Kathleen M. "Social Cybersecurity: An Emerging Science." *Computational and Mathematical Organization Theory*, vol. 26, no. 4, 2020, pp. 365-381, https://doi.org/10.1007/s10588-020-09322-9. Accessed 6 Apr. 2024.

Macnish, Kevin, and Jeroen Van der Ham. "Ethics in cybersecurity research and practice." *Technology in society* 63 (2020): 101382.

McAlaney, John, Jacqui Taylor, and Shamal Faily. "The social psychology of cybersecurity." *Psychologist* 29.9 (2016): 686-689.