The role of a cybersecurity consultant in relation to the social sciences

Sebastian Stovall

Cyse201

Professor Yalpi

Introduction

A cybersecurity career that relates to the principles of cybersecurity and the social sciences is a cybersecurity consultant. A cybersecurity consultant is defined as someone who identifies problems, evaluates security issues, assesses risks, and implement solutions to defend against threats to companies' networks and computer systems. A cybersecurity consultants' main job is to work with the victims of cybercrimes in order to not only establish a clear understanding of what is happening, but also be able to help them learn from their situation and move on to recover from it. It is also important that a cybersecurity consultant is well educated on what could've possibly led to the victim suffering the attack.

Example 1: Routine Activities Theory

For example, say a business calls a cybersecurity consultant to conduct an assessment on the company's cybersecurity procedures they would then go in to consider how effective the company is at maintaining its cybersecurity hygiene. These tests usually result in simulated social engineering attacks on the company's employees to see if they know how to properly react to these situations. First of all, if the consultant is well diverged on routine activities theory, they would check to see if the three elements that cause crime are present in the company's sake, these being a suitable target, motivated offender, and lack of proper guardianship. If the consultant takes on the simulated role of motivated offender, they will look to see if the company lacks the proper guardianship and is a suitable target. The consultant would then inquire on possible security measures set out by the company, whether these be physical security measures to keep them out of rooms storing classified company information or digital security like being careful to restrict certain employee permissions, if the company lacks extensive security, or fails to have proper surveillance to catch possible cybercriminals, this will make the company a

suitable target. If the company also failed to have proper security guards in place, or people that know and inquire about the difference between an actual employee and an alleged cybercriminal would lead to a lack of proper guardianship. If the consultant can see that these three elements are present, this would allow them to help to company to correct their security measures to lessen the chances of their company becoming victims of an attack.

Example 2: Victimization and Victim Behaviors

For another example, say a person has already become the victim of a cyber-attack and look to a cyber consultant to give them advice on their possible next steps. The cyber consultant would need to be educated on the difference between victim precipitation and victim blaming. If the consultant where to start blaming the victim for the attack, said victim might become less receptive to learning how they can correct themselves in the future, however if the consultant can explain their actions that led to the victimization, instead of saying the victim is cause of the action, they can educate them in a more effective way.

Conclusion

Overall, the role of a cybersecurity consultant is very reliant on the consultant being aware of the social sciences, due to the constant need for them to understand how people think and feel to work with them. A cybersecurity consultant needs to be well aware of how human's interact in relation to cybersecurity in order to teach not only companies but individuals as well to keep their cybersecurity hygiene as good as possible. People in these roles contribute to society as they serve as the buffer between well trained experts in the infosec world and average people who don't know much about cybersecurity.