Jeffrey Dylan Powell
25 October 2024
CYSE 201S - Online

Cybersecurity Engineer

Technical and Social Skills

A career as a Cybersecurity Engineer presents a diverse range of challenges, requiring professionals to maintain expertise in both the technical aspects of cybersecurity and the intricacies of human behavior. Proficiency in complex security protocols, threat modeling, and risk assessment is essential, along with a thorough understanding of social engineering tactics and behavioral analysis to effectively mitigate risks. Cybersecurity engineers are responsible for safeguarding an organization's computer systems and networks against cyber threats. This role demands skills in social sciences, including collaboration and training, as well as strong analytical abilities and insight into the human factors that influence cybersecurity.

How it relates to the principles of Social Science and Society

When cybersecurity engineers design computer security systems, they must grapple with the human factors challenges that organizations face. Their unique ability to bridge technology and psychology gives cybersecurity engineers the authority to mold policies and regulations, thereby shaping the future of cybersecurity. "Understanding the different types of cyber attackers and their characteristics can help organizations prepare their workforce to better identify potential threats" (Camillo, Hess 7). Putting yourself in the shoes of cyber offenders helps understand their motives and how they may go about committing cyber crimes. "Employers need to consider the psychological levers that cybercriminals pull when they use human behaviors to trick employees into clicking on links and giving away passwords" (Camillo, Hess 8). When a cybersecurity engineer takes into account, and works to understand, the human rationale and desire behind a cybersecurity threat and attack, they are better positioned to develop a safeguard against these threats and attacks.

Jeffrey Dylan Powell
25 October 2024
CYSE 201S - Online

In addition to delving into the underlying motives of cyber offenders, it is equally crucial to explore the behaviors and reactions of victims within the digital landscape. Understanding how individuals navigate this complex environment can provide valuable insights into their experiences and vulnerabilities when faced with online threats. One aspect can be victim precipitation. “Victim precipitation theory, the first theory of victimization, contends that victims contribute to the criminal events that harm them, either through victim facilitation or through victim provocation” (Lasky). Cybersecurity threats prey on this type of behavior to more easily facilitate cyber crimes and it is imperative for cybersecurity engineers to not only recognize, but understand, how the victim precipitation theory contributes to the execution of cyber crimes. Human error within an organization still stands to be one of the largest cybersecurity threats to an organization.

Cybersecurity engineers are not just tech-savvy, they also have a solid understanding of criminology, the study of crime and criminals. This knowledge equips them to comprehend the behaviors and tactics of cybercriminals. By understanding how these individuals think and operate, cybersecurity professionals can better protect systems and prevent future attacks. This interdisciplinary approach to creating cybersecurity policies is not just important, it is intellectually stimulating and constantly evolving. Although these topics are typically studied from a criminology perspective, they are often interconnected. “Criminologists involved in studying cybercrime, many of their studies have focused on explaining cyber crime and cyber victimization. The most popular criminological explanations of cybercrime include neutralization theory, self-control theory, learning theory, and routine activities theory” (Payne). In an ever-changing society, where criminology studies have existed and cybersecurity issues are comparatively new, the combination of the two fields is rapidly growing and changing to battle

and protect against these unique crimes and attacks. Establishing a robust cybersecurity policy as a Cybersecurity Engineer necessitates considering various societal factors, including human behavior, psychology, and criminology.

Diversity and Marginalized Groups within the Career Field

Cybersecurity threats and attacks do not occur solely on one group of people. These threats and attacks affect members of every gender, cultural background, and population. A field where threats and attacks impact all requires an approach that can address the diverse needs and address the unique challenges of each group. The cybersecurity engineering profession is predominantly male. According to CareerExplorer.com, men outnumber women by 68%, with 58% of them being white males. Additionally, there is a significantly low percentage of Black, Indigenous, and People of Color (BIPOC) in this field. This lack of diversity can lead to challenges such as limited perspectives, a shortage of innovative ideas, and a tendency for everyone to draw from their own experiences and cultural backgrounds. In any industry, if the workforce is homogenous, the ideas, solutions, and advancements may primarily benefit that specific group. A lack of diverse perspectives, experiences, and ideas restricts an organization's ability to effectively address the needs of the country's diverse population.

Conclusion

The role of a Cybersecurity Engineer transcends technical proficiency, demanding a multifaceted understanding of human behavior and social dynamics. As cyber threats evolve, so, too, must the approach to cybersecurity, which requires a blend of analytical skills and empathy for the victims and perpetrators of cybercrime. By integrating insights from social sciences and criminology, professionals in this field can develop more effective strategies to combat threats and shape policies that reflect diverse perspectives. Promoting diversity within the cybersecurity

workforce is essential to foster innovation and ensure that solutions cater to a wide array of experiences and backgrounds. Ultimately, the intersection of technology and human behavior will play a critical role in crafting a secure digital environment, underscoring the need for a holistic perspective in the ongoing battle against cyber threats.

Jeffrey Dylan Powell
25 October 2024
CYSE 201S - Online

Works Cited

CareerExplorer. (2024, January 4). *Security Engineer Demographics in the United States*.https://www.careerexplorer.com/careers/security-engineer/demographics/#:~:text=The%20largest%20ethnic%20group%20of%20security%20engineers,Asian%2C%20making%20up%2010%%20and%209%%20respectively.

Lasky, N. V. Victim Precipitation Theory. 1-2.

https://doi.org/10.1002/9781118929803.ewac0517

Payne, Brian K. and Hadzhidimova, Lora, "Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections" (2018). Sociology & Criminal Justice Faculty Publications. 39.

https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1039&context=sociology_criminaljustice_fac_pubs

Camillo, M., & Hess, S. (n.d.). *Human cyber risk – the first line of Defence*. AIG.

https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/cyber-human-factor.pdf

https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/cyber-human-factor.pdf

Jeffrey Dylan Powell
25 October 2024
CYSE 201S - Online