Career Paper: Security Systems Engineer

Tia Warren

April 17, 2025

Introduction

Security systems engineers are responsible for managing and creating security tools and methods for protecting computers and networks. This is done in the form of assessments that establish a system's requirements, vulnerabilities, and potential threats. By analyzing these assessments, Security systems engineers can offer frameworks and plans for a company to use to ensure the safety of a system, along with guidelines and policies for company employees to follow. This position requires a great degree of not only technical knowledge, but excellent social skills and the ability to effectively communicate to other staff members on why certain policies and tools should be implemented for security.

Social Science Principles

Security systems engineers do vulnerability assessments to figure out what system settings on computers and network devices need to be changed to increase security, but they're also responsible for teaching employees and users as to why those settings need to be changed and followed. It is imperative that a security systems engineer uses empiricism, skepticism, and parsimony when making decisions on what is a threat to their system, and how to ensure users don't become attack vectors for those threats. They use skepticism by doing audits and evaluations of their systems with teams like pen-testers to ensure a system is truly secure, empiricism to look at the data of those tests and previous benchmarks to make a decision on how to reduce risk, and then parsimony to explain these risks in a clear and concise way to the average layman. This means social dimensions like critical thinking, communication, teamwork, and problem solving skills are vital for the teams that work with the security systems engineer. As Alsharida et al. states:

> One of the most significant challenges to maintaining a secure network is user behavior, which is critical in identifying security incidents and data breach events. Therefore, attention should be given to theories and models because they provide an excellent comprehension of human behaviors toward various technologies and services.

This shows how the most important factor in this process is ensuring that any user awareness or employee training program is effective and establishes good cybersecurity values in the end users, as humans are the biggest and easiest risk that can be used to get into a system. It's also important that security systems engineers create an environment that promotes cyber hygiene and actively interacts with employees of all levels. Triplett states, "If workers see that leaders are implementing good cybersecurity practices and are committed to working with employees to develop best practices, they will be motivated to improve their practices" (2022).

Marginalization

The cybersecurity field is struggling with a lack of diversity, where only 14 percent of cyber professionals are women, only 6 percent of cyber professionals are African American, and only 7 percent of cyber professionals are Hispanic (Osman et al., 2023). Due to the security systems engineer having such a communication heavy role where they need to work with others to evaluate the integrity of a company's system, it's necessary to be open-minded. By being open and friendly to team members of all backgrounds, a security systems engineer can have a better chance at getting a well-rounded review because the members feel welcomed enough to bring new ideas to the table. Security systems engineers also need to be open-minded when it comes to education levels of the employees they're managing. The average employee isn't going to understand the complexities of the systems that they use to do their work, and a security systems engineer can't assume or try to force employees to be on their level to meet security standards.

By keeping an open mind and accommodating to less tech savvy employees, they can reduce the efficacy of risks like phishing.

Career Connection to Society

The security systems engineer plays a vital role, as they lead incident management actions and maintain the policies of corporations and companies (Cyberseek.org). This means that they're involved in the chain of people who have to decide how to inform customers of any breaches that the company has suffered, and how the company should internally work to resolve said breach to return to normal operations. They're also responsible for managing security between affiliated companies, as vulnerabilities can occur through a second party failing to do their part of security. This means they have an intimate connection to the social forces like wealth, the economy, and the media, as all three factors are affected by a company's response to a breach. Major companies can lose millions if they experience a data breach, and according to the journal article "Data Breaches: Financial and Reputational Impacts of Vulnerabilities on Organizations to Enhance Cybersecurity Strategies," major companies like Equifax, JP Morgan and Chase, and Target can experience notable stock price decline for several days to months due to a data breach, not to mention the losses in payments and reputation (A. Gite et al., 2024).

Conclusion

The security systems engineer not only assesses a system for technical vulnerabilities, but also for human-centered vulnerabilities. They must treat policy and procedure seriously, and communicate the requirements properly to any end-users within the organization to reduce the risk of breaches and incidents. This requires a proficient degree of communication with any teams and individuals involved in the process of evaluating systems and making policies. Furthermore, a security systems engineer must cooperate with teams that handle public relations

and communications with affiliated companies, as handling incident responses is a key action they must take.

Works Cited

A. Gite et al., "Data Breaches: Financial and Reputational Impacts of Vulnerabilities on Organizations to Enhance Cybersecurity Strategies," 2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2024, pp. 684-689, https://doi.org/10.1109/ICACRS62842.2024.10841577

Alsharida, R. A., Saleh Al-rimy, B. A., Al-Emran, M., & Zainal, A. (2023, April 28). A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society, 73. https://doi.org/10.1016/j.techsoc.2023.102258

Cyberseek.org. (n.d.). Cybersecurity Career Pathway. Cyberseek. Retrieved April 17, 2025, from https://www.cyberseek.org/pathway.html

Indeed Editorial Team. (2025, March 3). 15 Careers in Cybersecurity. Indeed. Retrieved April 17, 2025, from https://www.indeed.com/career-advice/finding-a-job/career-in-cyber-security

Osman, M. C., Namukasa, M., Ficke, C., Piasecki, I., & OConnor, T. (2023, October). Understanding How to Diversify the Cybersecurity Workforce: A Qualitative Analysis. Journal of Cybersecurity Education, Research & Practice, 2023(2). https://doi.org/10.32727/8.2023.23

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2(3), 573-586. https://doi.org/10.3390/jcp2030029