Diane Gilzow

CYSE 201S

April 17, 2025

Security Analysts and Social Science

BLUF: A security analyst is responsible for monitoring, detecting, and responding to cyber threats. They ensure that an organization's systems and networks are protected. Security analysts also apply social science principles in their field of work since a lot of cybersecurity often involves understanding human behaviors and actions.

Introduction

Cybersecurity is a field that involves more than securing the networks and systems that operate an organization, it also depends on the users and their behavior. Social science principles apply to the field of cybersecurity more than people realize because the field is centered around how people handle confidential data and how they interact with it. One cybersecurity profession where social science plays a significant role is that of a security analyst. By being a security analyst, it is important to understand social engineering, human behavior, and human-centered cybersecurity. With these facts in mind, security analysts can better design security protocols and user training that focuses on the human factor.

The Dangers of Social Engineering

According to Carnegie Mellon University (CMU), social engineering is the "...tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information." (University). Additionally, social engineering also takes advantage of human psychology to trick users into giving away sensitive information (University). A security analyst should be aware of social engineering tactics because these techniques specifically target the human mind rather than exploit technical flaws. Understanding social engineering can help security analysts better anticipate and recognize signs of social engineering attempts, such as not trusting unknown email attachments that are from unknown email addresses. Having awareness is a strong defense against social engineering and helps security analysts develop more effective security protocols and responses.

Human Behavior and their Associated Risks

Security analysts must understand how important human behavior is when it comes to cybersecurity. Humans are not perfect beings and are prone to making mistakes, which can lead to vulnerabilities arising within an organization. As mentioned earlier, social engineering is one of the most common ways attackers exploit human weaknesses, especially when it comes to the human mind. Humans possess many traits that could pose a threat to an organization's security, such as negligence or lack of awareness. An article from Forbes states, "We're on autopilot about 95% of the time. When it comes to preparing employees to be on the front lines in defense against cybersecurity threats, being on autopilot is not a good thing." (Carpenter). Since human nature needs to be taken into account, security analysts must recognize that people often rely on their habits rather than good decision making. Security analysts themselves must also stay vigilant, since they are mainly responsible for overseeing systems and networks. It is ultimately individuals who handle cybersecurity protocols, therefore, they must be able to communicate, possess critical thinking and problem solving skills, and most importantly, have good decision making skills.

The Benefits of Human-Centered Cybersecurity

Adopting a human-centered cybersecurity framework into an organization can help improve cybersecurity practices and an organization's security. By implementing a human-centered cybersecurity approach, it can help reduce human errors and improve business functionality. Security analysts should review and analyze frameworks that address the human factor, most notably the NIST Cybersecurity Framework. According to the Federal Trade Commission, "The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data." (Nguyen). The Federal Trade Commission points out that the NIST cybersecurity framework focuses on best practices for organizations that can help improve their cybersecurity (Nguyen). With the NIST Cybersecurity Framework, security analysts can utilize it to help implement defense mechanisms that not only address technical vulnerabilities but also account for human behavior and decision making. For instance, when it comes to protecting systems, security analysts can find ways to implement user training, role access, or user-friendly controls that can help reduce the potential risk of human error.

Marginalized Groups and Society

Security analysts may also engage with marginalized groups in society. Marginalized groups may not have as much access to cybersecurity education or knowledge, therefore making them more susceptible to facing a threat or attack. This lack of access can often be a result of systemic inequalities or lack of digital resources. Additionally, because marginalized groups may not have as much digital literacy as others, there may be bias when it comes to security policies that expect users to possess “average” cybersecurity knowledge. Low income communities may not have as much reliable Internet or computer software than others, which makes their systems more insecure and vulnerable to attacks. Since not every group has a privilege to basic cybersecurity controls, security analysts can help promote more inclusive cybersecurity policies and programs that can help provide more accessible cybersecurity training or tools. Security analysts ultimately help protect systems and data, but they can also help individuals build better cyber awareness.

Conclusion

Security analysts play a major role when it comes to protecting an organization’s data, systems, and networks. Their primary responsibility involves protecting and monitoring systems, data, and networks for an organization. Although the job is very technical, social sciences also apply to it. Social engineering, human behaviors, and human-centered cybersecurity all play a major role in promoting a well-rounded security infrastructure within an organization that can address both technical and human vulnerabilities. Technical vulnerabilities appear every so often, but the root cause, and often the solution, ultimately stems from humans themselves.

References

Carpenter, P. (2024, August 12). *Cybersecurity: What can we learn from the social sciences?*. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2022/06/24/cybersecurity-what-can-we-learn-from-the-social-sciences/

Nguyen, S. T. (2022, October 6). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

University, C. M. (n.d.). Social Engineering - Information Security Office - Computing Services - Carnegie Mellon University. https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html#:~:text=Baiting:%20A%20type%20of%20social,attachment%20with%20an%20enticing%20name

U.S. Bureau of Labor Statistics. (2024, August 29). *Information security analysts*. U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-2