Cybersecurity Professional Career Paper: Cyber Security Analyst

Student Name: Aiden Johnson

School of Cybersecurity

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/16/25

Cyber Security Analyst

A Cyber Security Analyst performs many tasks in their job, including planning, implementing, and upgrading their controls and measures (Surya et al., 2023). Their role is to monitor the network and ensure there are no security issues. The reason cybersecurity is so vital in the modern world is that everything is online to include your personal and financial data. You do not want to share your Social Security number or where you live with anyone. Without cybersecurity, this data would be vulnerable, and someone could just access a company's database and steal your information. This situation can become a serious problem for the company and the privacy of the people who trust the company. This paper will discuss the cybersecurity analyst's role, challenges women face in entering the cybersecurity field, and why cybersecurity plays a significant role in Society.

Social Science Principles

A cybersecurity analyst has a rewarding and fun career. Their success depends not only on their skills, but also on understanding human behavior. Their job is to detect cyber-attacks and determine why people fall for them. They do this by thinking like the person who falls for the attacks (Dawson & Thomson, 2018). Principles such as the Big Five personality traits are also incorporated into cybersecurity. The article discusses how this point is used to determine where a person should work and whether they should work at a place they hate or agree with the company's points. For example, if someone doesn’t agree with a company's points or hates the company, it risks an insider attack (Dawson & Thomson, 2018). This can be worse than an outsider attack, as all an insider has to do to steal the company's data is to insert a flash drive into the computer and copy the data onto it. A cybersecurity analyst has a combination of technical

skills and social intelligence to understand the computer network and the people with access, to keep it safe.

Dawson & Thomson (2018) found that situations influence how individuals act. For example, changes in a person's life, such as religious events or bureaucratic rules, can have a significant effect on their freedom (Dawson & Thomson, 2018). In contrast, a military officer will behave in the same way regardless of their role in the military. Someone without limits can think or act differently, raising more points and questions. (Dawson & Thomson, 2018).

Application of Key Concepts

A key concept discussed was the Big Five personality traits. But it is an excellent point in understanding why people think and do on the internet. The reason why these Big Five personality trait concepts are talked about is that, for a cybersecurity analyst, you have to understand these five traits as they provide a reasonable basis to start thinking about why some fall for an attacker, which is a good point to begin thinking neutrally. As a cybersecurity analyst, you have to think about a situation neutrally, don’t use options or what you may know, just stick to the facts of the attack. When you start thinking neutrally, you understand what is wrong and what needs to be fixed. Thinking neutrally means focusing on the facts rather than just guessing. It is also argued that companies should hire people based on their values rather than their skills (Dawson & Thomson, 2018). In other words, if you hire someone whose values match the company's, it can allow people to think more neutrally, rather than someone whose values disagree with the company's and can’t consider both sides of the situation.

Marginalization

In relation to cybersecurity careers and marginalized groups. Women face significant barriers when seeking jobs in STEM fields, including cybersecurity. There are a few reasons they struggle to get jobs in cybersecurity to include social expectations, family conflicts, a lack of role models in the field, and a lack of mentors (Giboney et al., 2023). Social stereotyping is a problem with people thinking they can't do the job or just not getting sponsorship. There are many more sponsorship opportunities for women to get jobs in cybersecurity. And a more social system for women in the field, too (Giboney et al., 2023). In addition, more companies are working to eliminate toxic work environments for women, removing stereotypes and providing training and skills to help them gain experience (Giboney et al., 2023).

Career Connection to Society

The ways that cybersecurity professionals contribute to the safety and stability of societal infrastructure are that they understand how to take care of vulnerabilities. Which vulnerabilities will always be a problem in any digital system. So, they use their skills and knowledge of digital security to keep the risk as low as possible. Cybersecurity professionals do not think about it in a company or society until a problem comes up. Cybersecurity professionals have to keep the CIA-Triad in place so that, if societal infrastructures like healthcare or financial systems get hacked, people's data doesn't breach confidentiality (Cavelty et al., 2023).

Conclusion

A Cyber Security Analyst plays a key role in the Cybersecurity field. They have a combination of technical skills, domain specific knowledge, and social intelligence (Dawson, 2018). They understand how attacks occur and how people fall for them. An analyst's goal is to

monitor the online environment and identify situations and people that make it easy to fall for these attacks. A cybersecurity analyst has to consider both sides of an attack to understand what is going on and to identify the facts. We also need to consider the broader side of the cybersecurity field. Women entering the career still face challenges in the field. Women can offer different perspectives about cybersecurity and offer different ways to approach situations. In that case, because women think differently, it may lead to finding a better solution to the problem. And with the digital age we live in, we have to think about cybersecurity's overall impact on society, as it is no longer just a company problem. Now, if an attack happens to an organization, we can not have access to fuel, cars, houses, or food. If this happens to our banking system, it can be devastating. Bank systems could be shut down because of an attack. Using your bank system would not work, so the only way you would be able to buy anything would be with cash.

References

Giboney, J.S., Anderson, B. B., Wright, G. A., Oh, S., Taylor, Q., Warren, M., & Johnson, K. (2023). Barriers to a cybersecurity career: Analysis across career stage and gender. *Computers & Security*, *132*, 103316–103316. https://doi.org/10.1016/j.cose.2023.103316

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, *9*(9). https://doi.org/10.3389/fpsyg.2018.00744

Cavelty, M. D., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research*, *26*(7), 801–814. https://doi.org/10.1080/13669877.2023.2208146

Surya, L., Patel, M., & Ravi Teja Yarlagadda. (2023). Current Trends in Information Technology. *Current Trends in Information Technology*, *11*(1). https://doi.org/10.37591/ctit