

Christopher Hilliard

April 14, 2026

Cybersecurity Career: Cybersecurity Analyst

Introduction

Cybersecurity has become really important today because almost everything we do depends on the internet. From banking to social media to even school systems, all of it needs protection. A cybersecurity analyst is responsible for keeping systems, networks, and data safe from cyberattacks and hackers. As technology continues to grow, the number of threats grows with it, which makes this job even more important. In this paper, I will explain how cybersecurity analysts use social science in their work, how concepts from class connect to this career, and how this field impacts different groups as well as society overall.

Social Science Principles in Cybersecurity

Cybersecurity is not just about technology—it also involves understanding people. A large number of cyberattacks happen because of human error rather than just technical weaknesses. For example, phishing emails are designed to trick people by creating a sense of urgency or fear so they give away personal information. Cybersecurity analysts study these behaviors to better understand how attacks work and how to prevent them (Hadnagy, 2018).

Another important part of the job is understanding how people interact with technology. If a system is too complicated or confusing, users are more likely to ignore security steps, which creates vulnerabilities. Because of this, analysts have to make sure systems are secure but still easy to use. They also help educate people on how to stay safe online, which shows how social science plays a role in real-world cybersecurity (Anderson & Moore, 2016).

Application of Key Concepts

One key concept from class that applies to this career is social cybersecurity. This focuses on the connection between human behavior and technology. Cybersecurity analysts use this idea to understand where risks come from, whether it is from external attackers or everyday user mistakes.

Risk assessment is another important concept. Analysts are constantly identifying possible threats and deciding how serious they are. Based on that, they put protections in place such as encryption, strong passwords, and multi-factor authentication to reduce those risks (Anderson & Moore, 2016).

Ethics is also a major part of the job. Cybersecurity analysts often deal with sensitive information, so they must make sure they are protecting data responsibly. They have to balance maintaining security while also respecting people's privacy, which can sometimes be challenging (West, 2019).

Marginalization and Cybersecurity

Cybersecurity does not impact everyone equally. Marginalized groups are often more vulnerable because they may not have the same access to technology or cybersecurity education. This can make them easier targets for scams and cyberattacks. In some cases, certain groups are even specifically targeted.

Cybersecurity analysts can help address these issues by improving accessibility and spreading awareness about online safety. There are also efforts to make the cybersecurity field more diverse, which helps bring in different perspectives and better solutions. Making cybersecurity more inclusive is important so that everyone can be protected, not just certain groups (West, 2019).

Career Connection to Society

Cybersecurity analysts play an important role in keeping society functioning properly. They help protect critical systems such as banks, hospitals, and government networks. If these systems are compromised, it could have serious consequences for a large number of people.

In addition, there are laws and policies that require organizations to protect user data. Cybersecurity analysts help ensure that companies follow these rules while also improving their security systems. Their work helps build trust in technology, which is something society depends on every day (Anderson & Moore, 2016).

Scholarly Sources

Research shows that human behavior is one of the main causes of cybersecurity breaches, which highlights the importance of social science in this field (Hadnagy, 2018). Other studies show that marginalized groups are more vulnerable to cyber threats, emphasizing the need for better protection and awareness (West, 2019). There is also research on cybersecurity policies and their role in protecting society, which connects directly to the responsibilities of cybersecurity professionals (Anderson & Moore, 2016).

Conclusion

Overall, being a cybersecurity analyst involves more than just technical skills—it also requires understanding human behavior. Social science plays a big role in how analysts prevent cyberattacks, make decisions, and protect users. This career also helps address issues related to inequality in technology while protecting important systems. Cybersecurity analysts are essential not only for organizations but for society as a whole.

References

Anderson, R., & Moore, T. (2016). The economics of information security. *Science*, 314(5799), 610–613.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Wiley.

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, 58(1), 20–41.