# Cybersecurity Professional Career Paper: Cybersecurity Analyst as a Social Science–Driven Career

Rieco Hellams
School of Cybersecurity, Old Dominion University
CYSE 201S: Cybersecurity and Social Sciences
Instructor Name: Professor Yalpi
Date: November 14, 2025

Cybersecurity is one of the most important careers in today's world because almost everything we do involves technology. Cybersecurity protects private information, computers, and the online systems that people and businesses use every day. Even though many people think cybersecurity is only about technology, it also has a lot to do with understanding people. Cybersecurity workers need to know why people make certain choices online, why some groups are more at risk, and how human behavior causes problems. This essay focuses on the job of a cybersecurity analyst and explains how social science helps them do their work, how they make decisions, and how they help keep everyone safe online.

Cybersecurity analysts use social science to understand why cybercrimes happen and why people fall for online scams. Research in psychology and criminology shows that people hack for many reasons, such as money problems, curiosity, peer pressure, or even political beliefs (Holt, 2023). Knowing this helps analysts predict what kinds of attacks might happen and who might be targeted. Analysts also study how people behave when they are stressed or rushed. For example, phishing attacks work because they make people feel scared, confused, or hurried. As Redmiles (2019) explains, people are more likely to click dangerous links or share private information when they feel overwhelmed. By understanding this, analysts can create better training that teaches people how to recognize fake emails and scams.

Social science also helps analysts understand how different people use technology and how culture affects the way people judge online risks. This is important when making rules, safety guides, and communication plans that everyone can understand. Cybersecurity analysts need to think about more than just computers—they also need to think about people. This shows that cybersecurity is not only about protecting systems but also about educating and guiding users.

Many ideas we learned in class connect to the daily work of cybersecurity analysts. Human error, trust, persuasion, and digital ethics all matter when analysts decide how to protect systems. Knowing how social engineering works helps analysts understand the tricks attackers use. Analysts also use the CIA Triad—confidentiality, integrity, and availability—to find weaknesses and plan solutions. Ethics are also important because analysts must protect people but also respect their privacy. When analysts monitor systems or check user activity, they have to think about how their actions affect trust and whether they are being fair.

Cybersecurity analysts also have to think about how online dangers affect certain groups more than others. Some people are more at risk for scams or identity theft because they have less access to technology, do not speak English fluently, or cannot afford strong digital protection. This is called digital inequality. Attackers sometimes target these groups on purpose because they think they are easier victims (Kraemer-Mbula et al., 2022). Analysts try to create safety guides that are easy to understand for everyone, no matter their background.

Sometimes, cybersecurity can even make unfair situations worse. Certain technologies, like facial recognition, make more mistakes with people of color or people from low-income neighborhoods. Ethical analysts work to stop this by supporting fairer laws and trying to reduce bias. They also work to make the cybersecurity workforce more diverse, so people from different communities can help make better decisions for everyone.

## Conclusion:

Cybersecurity analysts are extremely important for keeping society running. They protect schools, hospitals, banks, and government buildings from online attacks that could shut things down. Their work helps keep the public safe and supports national security. They also help

organizations follow important rules like HIPAA, FERPA, and NIST. Since so much of our daily lives depends on technology, analysts help protect the systems we rely on every day.

Even though cybersecurity is based on technology, social science plays a huge role in making it successful. Analysts use research on human behavior, online tricks, inequality, and ethics to make better decisions and create safer online spaces. Their work affects individuals, communities, and society. As online threats continue to change, cybersecurity analysts will always be needed to help make the internet safer and fair for everyone.

References

1. Holt, T. J., & Bossler, A. M. (2014). *Cybercrime*. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of Criminology and Criminal Justice* (pp. 1998-2009). Springer. https://doi.org/10.1007/978-1-4614-5690-2_211 Georgia Southern Commons+1
2. Redmiles, E. M., Mazurek, M. L., & Dickerson, J. P. (2018). Dancing Pigs or Externalities? Measuring the Rationality of Security Decisions. *Proceedings of the 2018 ACM on Economics and Computation* (EC '18), 211-228. https://doi.org/10.1145/3219166.3219185 ACM Digital Library
3. Leukfeldt, R., & Holt, T. J. (Eds.). (2019). *The Human Factor of Cybercrime.* Routledge. https://doi.org/10.4324/9780429460593 Taylor & Francis