Carter Wood

Career Paper

CYSE 201S

17 April 2025

How Cybersecurity Analysts Use Social Science Every Day

BLUF: *Cybersecurity analysts rely heavily on social science to understand human behavior, prevent cyber threats, and protect vulnerable communities. By applying psychology, sociology, and criminology, they not only secure systems but also ensure cybersecurity is fair, inclusive, and people-focused.*

Introduction

When people think about cybersecurity, they usually imagine code, firewalls, and hackers. But behind every data breach or scam is a human decision—and that's where social science comes in. One cybersecurity role that really blends technical skill with social insight is the **Cybersecurity Analyst**. These professionals don't just protect networks; they also study human behavior to predict and prevent cyber threats. This paper looks at how cybersecurity analysts apply ideas from psychology, sociology, and criminology in their work, especially when dealing with vulnerable communities and the broader public.

Why Social Science Matters in Cybersecurity

A big part of a cybersecurity analyst's job is figuring out how people fall for scams like phishing emails. That's where **psychology** comes in. Many attacks play on emotions—like fear, curiosity, or urgency—to trick someone into clicking a bad link or giving away sensitive info.

Analysts use this knowledge to train users and create better warnings to catch those moments before a mistake happens (Hadnagy, 2018).

Sociology also plays a role. One useful idea analysts use is **routine activity theory**, which says crimes happen when three things come together: a motivated offender, a target, and no one to stop it. Cybersecurity analysts use this concept to spot where systems might be vulnerable and step in as that "guardian," especially in places like schools or small businesses that might not have strong protection (Yar, 2005).

Criminology helps analysts understand who cybercriminals are and what drives them—whether it's money, politics, or revenge. That's important when it comes to defending people who are often targeted online, like LGBTQ+ groups, activists, or journalists. If analysts can recognize patterns in how and why these attacks happen, they can stay a step ahead.

Supporting Marginalized Communities

Cybersecurity analysts also play a big role in protecting groups that are more likely to be targeted online. Marginalized communities often deal with things like online harassment, surveillance, or doxxing. Analysts need to make sure their systems don't have hidden biases that ignore these risks or make things worse. Social science research—like studies on how tech impacts different communities—helps them do that (Eubanks, 2018).

Another key part of the job is **communicating risks** clearly. A lot of people don't have a tech background, and that's especially true in underserved communities. Analysts often need to break down complex threats into simple steps regular users can understand. They may also work with teachers or community leaders to spread security awareness in a way that actually connects with people.

Conclusion

At the end of the day, cybersecurity isn’t just about technology—it’s about people. Cybersecurity analysts rely on social science to understand how users think, how attackers behave, and how to protect communities fairly. The job takes both technical skill and human insight. As more of our lives move online, this blend of knowledge will be more important than ever—especially to keep everyone safe, not just those with the best resources or strongest systems.

Works Cited

Eubanks, Virginia. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press, 2018.

Hadnagy, Christopher. Social Engineering: The Science of Human Hacking. Wiley, 2018.

Yar, Majid. "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory." European Journal of Criminology, vol. 2, no. 4, 2005, pp. 407–427.