\

Cybersecurity Professional Career Paper: Life of a Risk Analyst

Student Name: Akela Villegas

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

November 15, 2025

Abstract

Cybersecurity today is not just about stopping malware or blocking hackers; it is about understanding the people behind those attacks and the people using the systems we are trying to protect. One of the roles that demonstrates this connection clearly is the Cybersecurity Risk Analyst. These professionals evaluate threats, study human behavior, and help organizations make smarter decisions about their security. This paper explores how social science principles shape the daily work of Cybersecurity Risk Analysts, how key concepts from the class support the profession, and how this career intersects with both society and marginalized communities who bear a disproportionate share of cyber harm.

Social Science Principles in the Risk Analyst Career

Cybersecurity Risk Analysts rely on social science far more than most people realize. In order to understand cyber incidents, one requires an understanding of human behavior. For example, research shows that cybercriminals are often motivated by thrill-seeking, financial gain, revenge, or a desire for status, not just technical curiosity (Holt et al., 2022). By recognizing these motives, analysts can predict the types of attacks that might occur and are able to tailor their defenses accordingly.

Risk analysts also apply the human-computer interaction (HCI) principle. Users frequently choose convenience over security, click past warnings without reading them, or misunderstand instructions entirely. Cranor (2008) explains that many secure systems fail not because the technology is weak but because humans in the loop are overloaded, confused, or poorly supported. Analysts use this kind of HCI perspective to evaluate how users actually

interact with security controls. Instead of blaming users, the analyst can recommend clearer warnings, better defaults, or less intrusive security steps.

Application of Key Concepts

Human-centered cybersecurity emphasizes that cybersecurity must be designed around human behavior, not just technology. The course material explains that many cybersecurity failures occur because tools, interfaces, and procedures do not match how people think, work, or make decisions. An analyst uses this concept when identifying whether a control makes the job harder for employees, which can increase human error, or if a step in a security process is too complex. By evaluating technology through a human-centered lens, analysts can recommend solutions that users will actually adopt, reducing the likelihood of human-enabled errors.

Another course concept is risk perception, which explains that people often misunderstand cyber risks due to bias, a false sense of safety, or habit-driven behavior. Analysts encounter this regularly: employees often underestimate phishing risks, click unsafe links out of routine, or reuse passwords because they assume nothing bad can happen. Understanding these psychological tendencies helps analysts design training, awareness campaigns, and policies that directly address human biases.

Marginalization

Cybersecurity challenges disproportionately affect marginalized communities. Individuals with limited digital literacy, financial instability, or inconsistent access to secure devices often face higher rates of fraud, identity theft, and online harassment. Research shows that cybercrime imposes heavier costs and consequences on these groups (Anderson et al., 2013). Analysts must consider these disparities when making recommendations. For example, they may

advocate for simplified authentication methods for users who cannot afford advanced devices or recommend training materials to those of lower levels of technical expertise.

Career Connection to Society

Analysts help protect essential systems that society relies on daily, including hospitals, financial institutions, universities, and government services. A single overlooked risk can disrupt critical infrastructure, compromise sensitive data, and impact entire communities. By identifying vulnerabilities early, analysts prevent incidents that could cause final harm, loss of public trust, or reputational damage.

Conclusion

The Cybersecurity Risk Analyst profession sits at the intersection of technology, criminology, psychology, and human behavior. Their work relies on understanding why offenders attack, how users interact with systems, and how social factors shape both risk and vulnerability.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M. J. G. van, Levi, M., Moore, T., & Savage, S. (2013, November 29). *Measuring the cost of Cybercrime*. University of Edinburgh Research Explorer. https://www.research.ed.ac.uk/en/publications/measuring the-cost-of-cybercrime/

Cranor, L. F. (2008). *A framework for reasoning about the human in the loop.* USENIX. https://www.usenix.org/legacy/event/upsec08/tech/full_papers/cranor/cranor.pdf

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2022). Cybercrime and Digital Forensics: An Introduction (3rd ed.). Routledge. https://doi.org/10.4324/9780429343223