Cybersecurity Professional Career Paper: Intrusion Analyst

Josiah Lynch

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Veereswara Lakshmi Diwakar

April 13, 2026

Introduction

Cybersecurity is a big part of everyday life now because almost everything people do is online. From banking to school accounts, a lot of personal information is stored on systems that can be targeted by hackers. One important career in this field is an intrusion analyst. An intrusion analyst is a cybersecurity professional who monitors network traffic in real-time to detect, analyze, and mitigate security breaches and unauthorized activity. They usually work in a security operations center and deal with real time alerts. This paper will explain how intrusion analysts use social science concepts, how ideas from class connect to their work, and how this career impacts society and different groups of people.

Understanding Human Behavior in Cybersecurity (SSP)

Intrusion analysts work with technology but their job also depends a lot on understanding people. Many cyberattacks happen because of common human mistakes, like clicking phishing links or reusing weak passwords, or anything likewise and because of this, analysts try to understand why people make these mistakes, which connects to social science ideas about behavior and decision making (Advanced social engineering attacks, 2015).

For example, phishing attacks are designed to create fear or unsureness so people react without thinking and click something mindlessly. Intrusion analysts look at these patterns and help organizations improve training so employees don't fall for them. Also system design matters, if something is too confusing people are more likely to mess up. Research shows that building a strong cybersecurity culture can reduce these risks by shaping how people behave online (Alshaikh, 2020) and a strong cybersecurity culture is that employees don't fall for

phishing emails easily, People use strong passwords and things like multi-factor authentication, Workers report suspicious activity instead of ignoring it, Security rules are followed naturally and not forced. So overall, intrusion analysts have to focus on both people and technology to be able to do a strong job.

Using Class Concepts in Real Situations (AKC)

Some key concepts that apply to intrusion analysts are empiricism, parsimony, and social cybersecurity. Empiricism is important because analysts rely on real data every day. They monitor logs, alerts, and network traffic to figure out what's happening and respond to threats based on evidence. Parsimony also matters because simpler systems are usually more effective. If security systems are too complex, users might ignore them or make mistakes. Intrusion analysts help make sure security measures are strong but still easy to follow.

Social cybersecurity is one of the most important concepts in this job. A lot of attacks involve human behavior, not just technical weaknesses. According to the Verizon (2023) report, many data breaches involve some form of human error. This shows why intrusion analysts need to focus on both technical systems and human actions when protecting organizations.

Unequal Risk and Digital Protection (Marginalization)

Cybersecurity can affect different groups in different ways, some people may not have as much access to technology or cybersecurity education which makes them more vulnerable to scams and attacks when on technology. For example, older adults or lower-income communities may not recognize phishing attempts as easily because they don't have access to technology. Intrusion analysts help organizations think about these risks and try to create protections for all users that would mitigate these concerns of risk. There are concerns about privacy and surveillance, especially for marginalized groups who may already face unfair monitoring.

Research shows that data and surveillance systems can sometimes increase inequality if they are not designed carefully (West, 2019) and that's because cybersecurity professionals need to consider fairness when building and protecting systems.

Protecting Systems and Society(CCS)

Intrusion analysts are important and play big roles in protecting society by defending important systems. Important systems like banks, hospitals, and government networks, which are critical for everyday life and if these systems are attacked, can cause serious problems for a large number of people.

They also help organizations follow cybersecurity policies and standards. The National Institute of Standards and Technology (NIST) provides guidelines for intrusion detection systems, which Intrusion analysts use in their work (NIST, 2022). By following these guidelines, analysts help prevent attacks and respond quickly when something goes wrong. Their work helps maintain trust in digital systems and keeps society running smoothly.

Research That Supports the Career (SJA)

One article explains how social engineering attacks work and how they take advantage of human behavior (Advanced social engineering attacks, 2015). This is important for intrusion analysts because they deal with these types of threats regularly. Another source discusses how organizations can build a cybersecurity culture to influence employee behavior and reduce risks (Alshaikh, 2020). This connects to how intrusion analysts help train users and improve awareness. A third source, the Verizon (2023) report, shows that human error is a major cause of data breaches. This supports the idea that intrusion analysts need to focus on both human and technical factors.

Conclusion

In conclusion, intrusion analysts are an important part of cybersecurity because they help detect and respond to threats before they can even happen, preventing damage. Their work depends not only on technical skills but also on social science principles like understanding basic human behavior concepts, such as empiricism, parsimony, and social cybersecurity all play a role in what they do. They also help protect society and consider how cybersecurity affects different groups. This career shows that cybersecurity is not just about technology but also about people.

Works Cited

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

National Institute of Standards and Technology. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (Special Publication 800-94). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Verizon. (2023). *2023 data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

nscdsnjndsjvndsjnvjdsnvjdsnjvndsjvnjdsnv