Cybersecurity Professional Career Paper: Incident Response Specialist

Keyshawn L. Braxton
School of Cybersecurity, Old Dominion University
CYSE 201S: Cybersecurity and the Social Sciences
Yalpi
April 14, 2026

Introduction

Most people think cybersecurity is all about firewalls and code, but it's more so about understanding people and how they operate. As cyber threats continue to grow, Incident Response Specialists have become essential to protecting global infrastructure. This paper examines the incident response career through a social science lens, exploring how human behavior, social inequality, and public trust all play critical roles in managing cyber breaches.

BLUF (Bottom Line Up Front)

Being an effective Incident Response Specialist requires understanding human behavior and applying social science principles just as much as technical skills. By using criminology frameworks and addressing challenges faced by marginalized communities, incident responders protect both the digital economy and the public trust that holds society together.

Social Science Foundations

Incident response depends heavily on psychology and sociology to understand attack motivations and human reactions during crises. When a breach happens, responders don't just patch servers, they also manage employee panic, communicate under pressure, and reconstruct the attacker's thinking. Heartfield and Loukas (2016) make it clear that social engineering exploits psychology, not software. This proves that cybersecurity is basically a social science, focused on how humans interact with technology and each other during stressful situations.

Application of Key Concepts

Several core concepts from this course apply directly to incident response work:

1. Routine Activities Theory: Responders analyze the three elements of any successful attack. These three elements are a motivated offender, a suitable target, and the absence of protection. Understanding this helps prevent future incidents.

2. Deterrence Theory: By implementing strict security protocols, responders create barriers that make the risk too high for potential attackers, discouraging them from targeting an organization.

3. Relativism: Different cultures have different practices around privacy and security. Responders handling international breaches need to account for these different views and perspectives.

4. Victim Precipitation: This framework helps responders understand how unintentional employee actions like clicking suspicious links can accidentally create openings that attackers exploit.

5. Social Engineering: The primary human factor in cybersecurity. Attackers use trust and authority to bypass technical defenses, making this a major concern for incident responders.

Impact on Marginalized Groups

Cybersecurity doesn't affect all populations equally. The incident response field faces several challenges related to marginalization. First, digital redlining leaves lower income communities with inadequate security resources, making them more vulnerable to identity theft and data breaches. Second, the lack of diversity in cybersecurity can create blind spots where security tools fail to protect users from different backgrounds. Third, bias in automated security systems often unfairly flags minority groups due to biased training data (Noble, 2018). Finally, language barriers in security training leave non-native speakers more sat risk to phishing attacks, creating higher risk distribution.

Career Connection to Society

Incident Response Specialists function as digital first responders. By protecting critical infrastructure in banking, healthcare, and government, they prevent systemic failures that would tarnish public confidence in essential institutions. NIST's incident handling framework (2012) has become the baseline for maintaining economic stability after major attacks. Beyond immediate response, these professionals shape public policy including mandatory breach notification laws that balance security needs with individual privacy rights.

Conclusion

The Incident Response Specialist role bridges technology and social science. By understanding the human element from attacker psychology to the impact on marginalized communities, these professionals do far more than repair technical systems. They protect the trust and stability that make up modern digital society.

****References****

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication, 800-61*.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR), 48*(3).

Noble, S. U. (2018). *Algorithms of Oppression*. NYU Press.