Myla Gorges

CYSE 201S

Professor Diwakar Yalpi

11/16/2025

Cybersecurity Incident Responders

INTRODUCTION

A cybersecurity incident responder is someone who specializes in identifying, analyzing, and weakening cyberattacks in real time. As online threats continue to increase, this career is very critical for protecting our personal data, company data, and natural infrastructures from damage. Even though the job focuses on technical skills a lot, social science research plays a crucially important role because most of the cyber incidents that happen often involve human error, decision making, human behavior, and social dynamics. This career paper will talk about how the social science principles support the work of our incident responders, how key concepts from our course apply to this career, how the profession acts with marginalized groups and how incident responders tend to contribute to society.

SOCIAL SCIENCE PRINCIPLES IN INCIDENT RESPONSE

Cybersecurity incident responders tend to rely deeply on all types of social science theories to help understand why cyberattacks happen and how people tend to behave during these attacks or incidents. Social science research helps explain the motivation behind hackers, insider threat behavior, emotional reactions to these incidents and the psychological pressure these hackers can create. The responders often analyze phishing attacks, social engineering attempts, and even user mistakes which each are shaped by these cognitive biases, the trust dynamics, and even social influences. Concepts from psychology, sociology, and more help guide policies for helping employees improve their awareness and reduce all types of risky behaviors.

APPLICATION OF KEY SOCIAL SCIENCE CONCEPS

Many different course concepts that we learn in class can apply directly to incident response work. For example, social engineering is one of the most common types of attacks that our incident reporters see on a everyday basis. Being able to understand these tactics like authority, urgency and social proof, can help responders easily spot and analyze when an individual is trying to manipulate others more often. Having concepts like risk perception, compliance behavior and threat modeling's are used when we want to evaluate how employers or employees can unintentionally cause breaches in a system. Responders are also applying psychological things when directing teams and restoring trust in one another at these companies after incidents happen.

MARGINALIZATION AND CYBERSECURITY

When it comes to cyber incidents, they don't impact all groups equally. When it comes to marginalized groups like low-income individuals, immigrants, and even individuals with limited digital literacy are the ones who are often at a greater risk. As an incident responder, it's important to understand how these types of inequalities are and how to respond to them appropriately and as well ethically. These groups are going to have fewer resources to recover from things like identity theft and scams that may be more vulnerable to social engineering. The cybersecurity teams are increasingly working to help develop inclusive, accessible training, and being able to diversify the field to improve representation throughout the field.

CAREER CONNECTION TO SOCIETY

When it comes to cybersecurity, incident responders are here to help protect society by securing places like hospitals, institutions, schools, and even government services. They tend to help maintain public trust in our digital world and can help prevent disruptions that are going to cause economic loss or even safety risks. They also tend to help shape policies in cybersecurity and can guide organizations towards safer digital practices that are going to benefit society.

CONCLUSION

The cybersecurity incident responder career combines technical expertise with social science principles. Responders are to apply psychology, social sciences, and behavioral research to get a better understanding of threats, communicate effectively with society and organizations, and support organizations during different types of cyber events. Their work can directly impact marginalized groups, making sure that fairness and accessibility are essential. Overall, incident responders play a vital role in society by protecting and supporting safe digital environments

REFERENCES

Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). A reverse digital divide: Comparing information security behaviors of Generation Y and Generation Z adults. International Journal of Cybersecurity Intelligence & Cybercrime, 3(1), 42–55. https://vc.bridgew.edu/ijcic/vol3/iss1/4/

Ghaleb, M. M. S., & Sattarov, A. (2025). Perceived security risks and cybersecurity compliance attitude: Role of personality traits and cybersecurity behavior. International Journal of Cyber Criminology, 19(1), 27–53. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/438

Hadlington, L. (2018). The “human factor” in cybersecurity: Exploring the accidental insider. Security Journal, 31(2), 1–17. https://irep.ntu.ac.uk/id/eprint/37590/1/14728_Hadlington.pdf