Cybersecurity Career Professional Paper: Cyber Threat Intelligence Analyst

Student Name: John Monrouzeau

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor name: Professor Diwakar Yalpi

Date: 11/14/2025

Introduction

The entirety of the cybersecurity profession plays a very vital role behind the scenes when it comes to protecting infrastructures, systems, and the public data of people. We are currently in a time where cyber attacks are the most complicated they have ever been, and can heavily be influenced by social and societal reasonings. So because of this, cybersecurity has become one of the most essential things for national security and public safety. This paper will go into depth as to how the specific career Cyber Threat Intelligence Analyst career professionals depend very greatly on social science principles to fully comprehend human behavior, analyze and comprehend threats, and to determine strong defensive strategies.

Social Science Principles: Relation to Career

A Cyber Threat Intelligence analyst depends on many social science research concepts to have an understanding as to why people and/or groups participate in malevolent cyber activities. The topic of criminology is often mentioned during such discussions, since it gives insights on usual motivations that hackers have, like financial debt, politics, societal pressure, or simply looking for an adrenaline rush (Holt et al., 2020). Psychology also helps analysts figure out behavior patterns of threat actors, and how even cognitive biases can push and alter their decision making skills. Another topic is sociology, which goes further into detail when talking about criminals and their groups and regulations within the group, as well as how having a feeling of social belonging can make its own impact on what hackers may do, too.

Social science principles go hand-in-hand with cybersecurity practices based on user behavior analysis and human-computer interaction. Cyber Threat Intelligence analysts use this information to see how users respond to misleading content online or phishing attempts. A good example of this would be how analysts base their training on behavioral science and studies to

get a stronger understanding that users are more capable of grasping more secure concepts of messages, like social belonging and emotional cues. These are used to make cybersecurity awareness strategies that specifically talk about user behaviors, which is done through phishing simulations, communication campaigns, and training regiments.

Application of Key Concepts

In class, we discussed several concepts related to the work that Cyber Threat Intelligence analysts handle in their day to day work lives, like risk assessment, policy compliance, human factor in security, and social engineering. Analysts use risk assessment to perceive and narrow down vulnerabilities that are in organizations by weighing out human actions and technical flaws, and how these things can lead to a bigger system threat. These include employee habits/routines and insider risks.

Marginalization

Cybersecurity greatly affects diminished groups in the cyber space because of uneven access to digital information, limited funding, and an overall higher risk of being exploited. Research has shown that marginalized groups usually have higher rates of cyber victimization because of systemic inequalities and reduced access to secure technologies (Vakhitova & Reynald, 2021). Cyber Threat Intelligence analysts have to keep these things in mind when creating threat reports and making programs to spread awareness. But professionals in the field aim to lower the statistics of these issues through methods of spreading information on the topics, and highlight policies that protect them. This is usually done by making training materials more accessible, proper communication skills, and making free security tools available.

Conclusion and Connection to Society

Cyber Threat Intelligence analysts make their contributions to the cyber space and society by having a positive impact on the stability and the protection of infrastructures that are within the public. They protect banks, hospitals, government networks, and other public resources from cyberattacks that could potentially cause major harm to a wide variety of people if someone with the wrong intentions had gained access to it. CTI analysts also push for organizations to agree with cyber laws that are implemented and put into place, like data protection regulations and requirements to report data breaches to the public. These laws and regulations also tie in to how CTI analysts are able to operate and carry out their jobs. By analyzing threats that occur in real time and giving advice to people on how to handle or counter it, CTI analysts play a strong and heavy role in the protection of the cyber space and the growing digital world overall.

Journal Articles

Source 1:

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2020). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

This source gives their ideas and theories about hacker motivation and digital criminal behavior, supporting the paper's discussion of how CTI analysts use criminology and psychology to understand potential cyber threats.

Source 2:

Décary-Hétu, D., & Dupont, B. (2016). The social structure of criminal networks on the Dark Web. *Global Crime, 17*(1), 1–21.

The article explains how cybercriminal communities function as social systems, supporting the analysis of sociological principles and marginalized group vulnerabilities.

Source 3:

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.

This source supports the discussion on how CTI analysts support society by monitoring political and social threats and contributing to national policy decisions.