# Cybersecurity Professional Career Paper: Cybersecurity Specialist

Student Name: Joseph Diep

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/8/2025

## Introduction

A cybersecurity analyst is an individual that is proficient in securing digital data, identifying vulnerabilities, and implementing prevention to ensure data remains confidential, holds integrity, and is available to be used. This field of cybersecurity is growing ever more important as we engage in significant digitalization of information. The information stored online can be personal identifiable information (PII) such as identification cards, social security number, date of birth, and any other personalized information that will give away your identity. Now, more than ever, malicious threats have gained unprecedented opportunities to capitalize on unsecure data that individuals rely on. Cybersecurity analysts are essential in defending information, developing incident response plans, and demonstrating how human behavior affects resilience to cyber threats.

## Social science principles

Although cybersecurity is deemed to be a technical role it also deals with social aspects as well. One such instance of cybersecurity being a social role Is dealing with the end-user the person in control of data or the malicious threat actor that seeks to exploit data. As cybersecurity professionals it is necessary to use ethical hacking to enforce a safer digital environment misuse of cybersecurity could result in the harm or improper intrusion of an individual’s data. Additionally, cybersecurity is a very human-centric field where mitigation strategies rely on educating the people about threats and proper technology usage. Peslak acknowledges said that “Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices.” (Peslak et al., 2019). Parsimony is a social sciences principle which can establish easier understanding of cybersecurity best practices. This principle simplifies instructions and terms to allow individuals that lack fundamental understanding of cybersecurity to follow procedures.

## Application of Key Concepts

Cybersecurity analysts are tasked to perform multiple functions within an organization to ensure security measures in defending against cyber threats. The skills necessary for this job position are often technical with experience related to technology, OS, networking, business management and soft skills in communication and presentation are also important for the job. Cybersecurity analysis might require some level of business management when coordinating with different departments of a company to help allocate costs in a business continuity plan (BCP). The BCP aligns with the skills of recovery plans ensuring different infrastructure required for operations are understood in an event of an incident (Thomas et al., 2018). BCP also connects with economics as it ensures companies are capable of recovering, in the event of an incident, to resume company operations to gain revenue and to protect wealth assets regarding potential banking information.

## Marginalization

Implementing cybersecurity is costly to maintain leaving organization with no choice but to accept some levels of risk to ensure financial stability. This is referred to as a cost benefit analysis. Some companies might lack the funding to fully secure their facility. As cybersecurity professionals there might be lack in different job sectors who are willing to accept cybersecurity services because of these costs. One such case is small to medium-sized companies which must pay employees higher on average salaries as opposed to larger corporations; while also having a significantly lower budget of $8,500 (frameworksecurity, n.d.). Cybersecurity experts suggest that companies do not need to obtain expensive cybersecurity services but to educate employees with cybersecurity training and make sure that Multifactor authentication (MFA) is used. In essence the weakest link, humans, are the ones that should be prioritized in securing a workplace.

## Career Connection to Society

Cybersecurity is crucial in a technology driven society to ensure that data and information remain confidential, holds integrity, and is always available to be used. Cybersecurity analysts secure many sectors of society from energy to hospitals. The health insurance portability and accountability act (HIPAA) is one mandate that ensures an individual's personal health information (PHI) is secured. Cybersecurity threats exploit valuable health information protecting such information is vital in health facilities to remain compliant with regulations and to ensure safety of health information.

## Conclusion

Cybersecurity analysts have multifaceted skill sets that are above just technical expertise and are used to secure data in various sectors. Cybersecurity analysts develop BCPs with communication and work with different departments to ensure a business can recover from an incident. These individuals working among health facilities and employees to ensure that PHI is confidential and that end users are trained in cybersecurity to mitigate the chances of becoming victims of cyber threats.

## Scholarly Journal Articles

- Peslak, A., & Hunsinger, D. S. (2019). What is cybersecurity and what cybersecurity skills are employers seeking?. *Issues in Information Systems*, *20*(2).
- Thomas, L., Vaughan, A., Courtney, Z., Zhong, C., & Alnusair, A. (2018, July). Supporting collaboration among cyber security analysts through visualizing their analytical reasoning processes. In *2018 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)* (pp. 1-6). IEEE.
- Abbasi, N., & Smith, D. A. (2024). Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 3(3), 278-287.
- How much does cybersecurity really cost?. Mar 24, 2025. (n.d.). https://frameworksecurity.com/post/how-much-does-cybersecurity-really-cost#:~:text=For%20small%20businesses%2C%20cybersecurity%20budgets,their%20IT%20budget%20to%20cybersecurity.