Cybersecurity Professional Career Paper: Cybersecurity Analysts

Student Name: Leyah Knox

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: 4/14/2026

Cybersecurity analysts are professionals when it comes to protecting computer systems, sensitive data from cyber such as phishing and hacking, and even networks. As technology gets a bigger wide span in our everyday life, cybersecurity has become essential for protecting people's personal information, national security info, and even some businesses information. Huge organizations like healthcare rely on cybersecurity analysts to maintain their systems and make sure they are secured. The purpose of my paper is to show how cybersecurity analysts rely on social sciences and their principles for their daily work life, and eventually my daily work life. Even though Cybersecurity can look like it's all about technology, it also has you understand human behavior, and their social systems that help you in the long run. My paper will explore how those social science principles contribute to cybersecurity practices.

Social science plays a huge role in helping cybersecurity analysts understand why people may engage in risky behavior online or even possibly commit a cyber crime. One example is that attackers most of the times use social engineering techniques that can exploit human psychology like trust and fear. Being able to understand these behaviors allows cyber analysts to prevent attacks more. Analysts use empiricism to rely on real world data like activity log ins, to identifying cyber threats. Objectivity makes sure that analysts get the measure of threats without being bias, and heavily only focused on evidence. Determinism I feel as though is a important one because it helps them predict patterns in people's behavior, meaning they can detect if someone is clicking phishing emails. Cybersecurity professionals use these principles on a day to day basis when doing these training programs and analyzing threats.

There are plenty of concepts from class that are essential in the cybersecurity career. One of them are human factors, which show that humans are often the weakest link in cybersecurity. Analysts use this concept to monitor user behavior and apply training programs so they can

reduce errors. Professionals use this concept by using tools such as security information, and user behavior analytics. This specific tool helps analysts monitor activities and identify threats while considering human behavior and some organizational risks.

One major concern dealing with marginalization is the digital divide to where people with limited access to technology or cybersecurity smarts are more vulnerable to being a cause of an attack. These may lack awareness of phishing scams or secure online practices. Another issue with this is cyber crime, where some marginalized groups are more likely to experience online harassment, identity theft, or even financial scams. Cybersecurity professionals are working to solve those challenges by promoting these practices. This includes them developing accessible cybersecurity knowledge programs, and supporting diversity with in the workforce. By doing this, analysts help to make sure everyone receives equal protection in the digital world.

Cybersecurity analysts play a big role in maintaining the stability and safety of society. They protect critical issues like financial systems, government networks, and healthcare organizations. Without effective cybersecurity those systems would likely be able to cause disruptions that could really affect a lot of people. Public policies that are related to cybersecurity like data protection laws and privacy regulations, also show how analysts do their job. These policies aim to protect people's information while making sure organizations follow their proper security practices. Cybersecurity professionals have to understand and abide by these regulations so it can balance security with everyone's rights. Cybersecurity analysts aim towards gaining public trust. When organizations continue to have strong security, people feel more confident using technology services. For example, online banking. Online banking is something people have to really put their trust in, because this is an account that has to do with all their assets. This shows strong connection between cybersecurity and societal trust.

- Source 1: Focuses on human behavior in cybersecurity incidents. It also highlights how users actions, such as falling for phishing emails significantly contribute to security breaches. This helps my idea that cybersecurity analysts have to understand behavioral patterns to be able to prevent attacks.

  - Ramezan, C. A., Ahmad, M. J., Schaupp, L. C., Hatten, F. W., & Starling, M. A. (2026). The modern cybersecurity analyst: An international position analysis. *Computers & Security*, *163*, Article 104825. https://doi.org/10.1016/j.cose.2026.104825

- Source 2: Shows organizations using cybersecurity practices and human factors. It shows how training and organizational culture influences some security outcomes, making the importance of social science principles show how effective they are in their cybersecurity careers.

  - Balogh, Š., Mlynček, M., Vraňák, O., & Zajac, P. (2024). Using Generative AI Models to Support Cybersecurity Analysts. *Electronics (Basel)*, *13*(23), 4718. https://doi.org/10.3390/electronics13234718

- Source 3: Explores a lot of social implications dealing with cybersecurity. Showing its impact on society and its contributes to understanding how cybersecurity professionals work considering the responsibilities and societal effects in their work.

  - Jiang, W. (2024). Cybersecurity Risk and Audit Pricing—A Machine Learning-Based Analysis. *The Journal of Information Systems*, *38*(1), 91–117. https://doi.org/10.2308/ISYS-2023-019

Cybersecurity analysts rely on social science research and it's principles to perform their roles amazingly well. Understanding human behavior and societal factors allows them to be able to predict and prevent on going cyber threats. The main concepts such as human factors, social engineering, and risk perception are all in everyday cybersecurity practices. Cybersecurity professionals play a huge role in addressing challenges and ensuring equal protection in digital space. As cyber threats continue to grow, the mixing of social science into cybersecurity will always be essential for building secure and digital future.