

Cybersecurity Analyst: A Career Analysis

By: Kayle Glaize

School of Cybersecurity

CYSE 201S Section 34568

Professor Matthew Umphlet

June 22 202

Technology has continued to advance and has become an integral part of daily life for most people, but with this integration, new threats have emerged. Cyberattacks are starting to become much more common as we've become more reliant on technology; these attacks get more frequent and complex with each passing day. To combat this, organizations in recent years have needed to hire cybersecurity professionals to protect critical systems and sensitive data from cyberattacks. Among the most important cybersecurity professions is cybersecurity analysis; their role comprises monitoring systems for potential weaknesses, maintaining security software, and investigating security breaches and cyberattacks. This role often requires strong technical knowledge and proficiencies; having technical expertise isn't necessarily enough to have a successful career in this field.

Hackers often target the human aspect of cybersecurity as opposed to facing the technological security head-on; this requires that professionals in this field have an understanding of human interactions and behaviors, psychology, and sociology. Additionally, because cybersecurity is just as much about protecting people as it is technology, having a grasp on how organizations can affect behavior, individual employee decision-making strategies, and social factors can impact security. The combination of social and technical sciences gives cybersecurity analysts the edge they need to develop effective security protocols and respond to security threats.

A cybersecurity analyst employs many different concepts from the social sciences, but among the most important is the concept of human factors. This kind of approach places people at the center of cybersecurity because they are the weakest link and thus understanding their behavior is key to improving security. Cybersecurity analysts use human factors by studying how employees interact with technology to identify habits and behaviors that can result in security

risks. For example, if they notice an employee using the same username and password across multiple systems, an analyst can look into ways to correct that behavior through different security measures or training. Research has shown that upwards of 72% of data breaches involved some sort of human element along the way, further reinforcing the idea that cybersecurity is a field heavily connected and reliant on human factors (ScienceDirect). Decision science and risk management are two other concepts that play large roles in this field. Security analysts and other cybersecurity professionals use decision science to make informed decisions rather than solely relying on their intuition. Analysts can use these skills to recommend and create new security protocols, conduct vulnerability prioritization, and evaluate threats. Risk assessment is also heavily used; security analysts use this concept to organize information on possible threats and vulnerabilities, allowing them to allocate resources or develop effective security controls and generally make more informed security decisions (National Academies).

Determinism is another principle that is often employed in this position. The idea of determinism is that every action or event was caused directly by previous identifiable events or actions. According to an article from the Non-Human Identity Management Group, oftentimes the occurrence of a security threat can be traced back to an identifiable event/s, such as a design flaw, human error, or even misplaced trust. A cybersecurity analyst can use the concepts of determinism to investigate the cause of an attack to better understand how it started and how to address the issue to prevent it from happening in the future (NHI).

Cybersecurity analysts play a critical role in protecting marginalized groups and society in general from digital threats. Lower-income communities, the digitally illiterate, the elderly, and other marginalized groups are all at a much greater risk of being targeted by cyberattacks

and scams such as phishing and identity theft. A cybersecurity analyst's job is to investigate vulnerabilities, create and implement stronger security measures, and provide education on digital literacy and safe security practices, making technology more accessible and safer for all people. Because technology is so heavily interconnected to most things, cybersecurity analysts also protect societal infrastructures like power grids, government agencies, and communication systems from cyberattacks while at the same time ensuring the people's personal data, like banking information and hospital records, are properly secured. Cybersecurity analysts work hard to protect the nation's infrastructure and defend the personal data of millions while ensuring both individuals and organizations alike can continue to safely use technology and the internet.

A cybersecurity analyst is a complex role that relies on more than technical knowledge to fight off cyberthreats. By implementing concepts from social sciences, such as psychology and sociology, and applying concepts like determinism, decision-making, and human nature, cybersecurity analysts can gain an understanding of how and why security incidents occur and how to prevent them in the future. As technology will continue to evolve, we will need to rely on security analysts more and more to ensure the sensitive data of the public and our nation's critical infrastructures remain protected.

Work Cited

Read. The National Academies Press. (n.d.).

<https://www.nationalacademies.org/read/24676/chapter/4>

Transforming threats into opportunities: The role of human factors in enhancing cybersecurity -
sciencedirect. (n.d.).

<https://sciencedirect.com/science/article/pii/S2444569X25000459?via=ihub%3D>

What is deterministic security? Definition & Examples. NHI Management Group. (2026, August 1).

<https://nhimg.org/glossary/deterministic-security/>