Samuel Woodruff

Professor Yalpi

11/24/2024

Career Paper

Cybersecurity Analysts and Social Science

Introduction

Our world is more interconnected now more than ever with the advancement of technology and the internet. With such interconnectedness, cybersecurity has taken on a massively important role in our society to protect privacy, infrastructure, and integrity. A prominent career in cybersecurity today is that of the cybersecurity analyst. Cybersecurity analysts can find work in all sorts of organizations and are extremely integral in the maintenance of systems and security. As one of the most common careers in cybersecurity, cybersecurity analysts are impactful not only for organizations but also for society as a whole. Similarly, they must utilize many social science principles and research for their field. Through all of this, cybersecurity analysts stand as one of the most multifaceted and important careers in the world of cybersecurity.

What is a Cybersecurity Analyst?

The cybersecurity analyst career is one of the most dynamic and multifaceted in all of cybersecurity. According to the University of Maryland Global Campus, the daily tasks of a cybersecurity analyst usually consists of "...monitoring security events, identifying threats, investigating incidents, and devising strategies to prevent future attacks" (UMGC, p1. 2024). Cybersecurity analysts may have more or less responsibilities depending on the organization. They are one of the most dynamic roles in all of cybersecurity in that the threats that they work to counter are constantly evolving.

How Social Science Principle/Research and Core Concepts are intertwined with Cybersecurity Analysts

A cybersecurity analyst must have great knowledge and understanding of social science principles and social science research to perform their tasks at a high level. Firstly, a cybersecurity analyst must research and investigate with objectivity in order to strictly advance knowledge. Likewise, cybersecurity analysts must conduct their research into their systems and breaches using empiricism. Cybersecurity analysts must use the principle of parsimony to keep their explanations and findings brief and to the point when presenting them to their respective organizations. Another principle cybersecurity analysts must use is relativism to help them understand new crime and potential security risks from the advancement of technology. Importantly, cybersecurity analysts must understand economic theories like Marxian Economic Theory to understand what might drive individuals to exploit an organization's weaknesses. As Tim Maurer and Arthur Nelson put it, "...the assessment that a major cyberattack poses a threat to financial stability is axiomatic— not a question of if, but when" (Maurer, Nelson, p.1, 2021).

Attacks on financial institutions are inevitable, so it is up to roles like the cybersecurity analyst to understand economic theories and their implications in order to better protect their organizations.

Marginalized Groups in regards to Cybersecurity Analysts

Marginalized groups face many challenges when it comes to cybersecurity as a whole as well as in careers such as cybersecurity analysts. Great strides have been made in the diversification of the cybersecurity field, but some groups remain underrepresented. As Ben Allen of SecureWorld writes, "...the percentage Black and Hispanic professionals in cybersecurity has seen a modest increase, the representation of Asian individuals remains disproportionately low" (Allen, p. 1, 2024). Asian individuals remain underrepresented in the cybersecurity field despite other groups seeing increases in representation. Ben Allen goes on to explain that another area of disproportionate minority representation is between urban and rural minority cybersecurity workers. Allen explains that urban workers tend to have better job opportunities and access to education which may explain the gap between urban and rural minorities in cybersecurity. Women also face an unjust barrier when it comes to landing a job like a cybersecurity analyst. While the percentage of women continues to grow in cybersecurity, there is still a considerable gap between male and female cybersecurity workers.

Cybersecurity Analysts connection to Society

Cybersecurity analysts are greatly connected to society and what keeps society as a whole running day-to-day. First, cybersecurity analysts help to protect critical infrastructure such as transportation, energy production, water purification, and much more. Cybersecurity analysts

also help to protect financial security of individuals and businesses. Lastly, they also help to safeguard national security to ensure the nation is properly defended and secure.

Conclusion

The cybersecurity analyst has many responsibilities that cover the day-to-day cybersecurity functions of a business or organization. They are responsible for protecting systems, devising mitigation strategies, investigating breaches, and much more. They must be able to use and understand many social science principles to efficiently perform their job functions. This career is crucial in providing security for much of what makes society run day-to-day, ensuring businesses, government agencies, and critical infrastructure are able to operate. As a whole, the career of a cybersecurity analyst plays not only a major role in cybersecurity, but also society at large.

Works Cited

Allen, B. (2024, June 2). *Minorities and the Cybersecurity Skills Gap: A 2024 update*. Cybersecurity Conferences & News. https://www.secureworld.io/industry-news/minorities-cybersecurity-skills-gap-2024

Maurer, T., & Nelson, A. (2021). *The global cyber threat to financial systems – IMF F&D*. IMF. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

What does a cybersecurity analyst do in 2024?. Online Tech Bootcamps. (n.d.). https://careerbootcamps.umgc.edu/blog/cybersecurity/what-does-a-cyber-security-analyst-do/