Jonathan Roeseler
November 24, 2024

Career Paper - Cybersecurity Policy Analyst

INTRODUCTION

A cybersecurity policy analyst is responsible for creating and developing appropriate, ethical policies to support an organization's initiatives and compliance. A policy analyst is accountable for converting technical measures into written words any human can understand – demonstrating parsimony ("Visual structures"). These policies must be developed without bias (objectivity and ethical neutrality), to ensure fair measures are in place for all involved. Additionally, policy analysts must have the ability to decipher data and research to develop the best policies possible (skepticism). A policy analyst requires an understanding of all the social science principles to effectively do their job. Not only must they stay up to date with cyber trends to develop policies reducing threats, but they must also understand how a certain policy may affect an organization, a specific group, or an individual's privacy.

KEY CONCEPTS

Cybersecurity policy analysts must be able to understand how psychology and cybersecurity correlate. Cyberpsychology stresses how human behavior and psychological states are influenced by technology. By understanding how people interact with technology, and analyzing psychological factors like fear and trust, an analyst can implement an effective cybersecurity policy addressing these factors, which many attackers seek to exploit. Another element an analyst must understand is the CIA triad. Confidentiality, Integrity, and Availability are the core components that must be addressed for an effective policy. Prioritizing a human-centered cybersecurity model is also the job of a policy analyst. A human-centered model is the best method for preventing the most common and successful attacks, social engineering, and phishing. Training users and understanding users' behaviors is a big part of an analyst's job. Finally, developing an organizational cybersecurity culture is necessary for a company to reduce risk. For example, this could be enforcing users to use MFA, not click on phishing emails, and recognizing social engineering attempts. All of this starts at the top, with effective policy, mandating proper training, rewarding users for reporting threats, and asking for help should they have a question.

MARGINALIZED GROUPS

A cybersecurity policy analyst's policies affect a wide range of users, and if an analyst neglects or overlooks a group from the policy, it can have disastrous effects (Deepika). Many policies disproportionately affect marginalized communities, which face several problems, such as privacy concerns, cultural sensitivity, and transparency. It is important privacy concerns are addressed and properly communicated (transparent) to its audience. Analysts must converse with different and diverse groups to understand the values of differing communities when writing an effective policy. An analyst should consider their policies from a Human Rights framework perspective, as it would allow the analyst to better understand the effects of their policy on all groups of people (Deepika).

CONNECTION TO SOCIETY

A cybersecurity policy analyst plays a critical role in shaping digital environments for a large number of people, demonstrating the large effects their policies can have on society. One of the main goals a policy analyst first seeks to address is educating users on what attacks they can expect on a normal day and how they can mitigate them – the most common being phishing and social engineering training. Analysts are also responsible for creating the cybersecurity culture, everything flows down from their policies. For example, mandating phishing awareness training and rewarding users for reporting threats fosters a strong cybersecurity environment, versus one that does not mandate training nor has its users report threats. According to Ling, rewarding and motivating users to complete training and report threats is necessary for an effective cybersecurity culture. Policy analysts are also crucial to ensuring a fair and safe environment for users. Including inclusive policies allows marginalized groups to have equal and safe access to resources, addressing the digital divide these groups face. Policies should be able to address every group's needs, and in an office's case, this includes remote versus in-office workers. According to Nwankpa and Datta, despite the disconnect between how the two groups feel about how safe they are (office workers are more likely to take risks as they feel safer at the office and behind the company firewall), it is necessary for a policy to be implement training for both so they understand the risks poised being in-office versus remote. Finally, policy analysts are responsible for creating policies that safeguard people's privacy and data, without an effective policy, users are subject to having their data exposed, leading to identity theft, fraud, and more malicious activities.

CONCLUSION

Cybersecurity policy analysts must foster inclusive and effective policies that protect all users, ensuring no group is vulnerable. By developing clear, transparent, and unbiased policies, an analyst can address the diverse needs of society. Staying up to date with trends is a necessary task for an analyst to keep policies up to date with current problems. Ultimately, well-crafted cyber policies safeguard the privacy and security of every individual in today's world, and it is a cybersecurity policy analyst's job to ensure this is done day-to-day as the digital world moves at a super fast pace.

References

Joseph K. Nwankpa, Pratim Milton Datta, "Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers," Computers & Security, Volume 130, 2023, 103266, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103266

J. Stoll and R. Z. Bengez, "Visual structures for seeing cyber policy strategies," *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, Estonia, 2015, pp. 135-152, doi: 10.1109/CYCON.2015.7158474.

Ling Li, et al., “Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior,” International Journal of Information Management, Volume 45, 2019, pp 13-24, ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Paira, Deepika. "ENSURING INCLUSIVITY IN CYBERSECURITY: A HUMAN RIGHTS-BASED APPROACH." *CYBER CRIME, pp. 95-*.