Cybersecurity Professional Career Paper: Cybersecurity Policy Analyst

Student Name: Bryce Baxter

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/13/25

Introduction

In today's world, the importance of a Cybersecurity Policy Analyst is only going to increase along with cyberattacks and the importance of the policies we have in place to protect all users. A cybersecurity policy analyst develops, analyses, and implements cybersecurity policies into organizations and the public to protect all users from cyberattacks. However, social science also plays a large role in this occupation. Psychology, Sociology, and even political science all play a role in developing and implementing cyber policies. In this paper, I will analyze the cybersecurity policy analyst occupation and how employees use social science research methods in their daily routine, how this job connects to our class in CYSE 201S, and how this job interacts with larger groups and society.

Social science principles

A basic insight from social science is that humans are integral to system security, in all phases of it. As users, operators, and even bystanders. The National Academies of Sciences, Engineering, and Medicine emphasizes that "technical approaches alone will not suffice, humans play roles in systems as developers, users, operators, or adversaries." In a cybersecurity policy analyst role, this means using social science research methods like psychology and sociology in your daily routine. For example, this could be people ignoring social norms, and cognitive biases.

Additionally, political science and policy studies are also important for the cybersecurity policy analyst position. Policy analysts must understand governance frameworks, power dynamics, stakeholder interests, institutional incentives and how policies may affect different groups of society. Finally, ethics and justice principles from sociology and philosophy come into play: when crafting policies a cybersecurity policy analyst must balance security imperatives with privacy rights, equity, and non-discrimination. Social science helps inform these ethical dimensions and prevents blind technological solutions.

Application of Key Concepts

In class, we have discussed concepts like relativism, empiricism, social structures, and behavioral influences in the cybersecurity world. A cybersecurity policy analyst uses these key concepts every day. For example, applying empiricism means using empirical research methods like survey data, and incident-report studies and not just technical speculation in your research. The analyst might utilize social science methods to assess how employees perceive risk or how different demographic groups respond to authentication policies.

Relativism is recognizing that social behaviors and institution designs may vary from person to person and organization and organization. A policy that works in one culture or organization may not translate to another due to different trust norms, authority structures or digital literacies. That is why it is important for policy analysts to be socially and culturally aware. Ethical neutrality demands that the policy analyst sees their role as impartial facilitator of evidence-based policy, not inserting bias or favoring certain groups without justification. For example, a analyst might test how a new multi-factor authentication policy impacts low-income users, the policy analyst will adjust the policy to avoid digital exclusion.

Lastly, behavioral science is also applied to new policies regularly in this profession. For example, if users choose to ignore authentication pop-ups that appear too often, then a policy analyst may come up with a policy to optimize frequency and presentation of authentication pop-ups in user friendly ways.

Marginalization

Typically, some policies may affect some marginalized groups in negative ways without any intention. A policy analyst must pay specific attention to how marginalized groups experience risk differently and how policies might widen existing inequalities. This is exactly why social science is so important. Social science helps show the similarities and differences between marginalized groups and how a new policy can benefit and negatively affect each group.

A cybersecurity policy analyst may do a analysis on how different groups interact with cybersecurity policies. Research methods like focus groups and surveys might be used to gather data from

those different groups. This allows the analyst to ensure that the policy is justified and socially just. This aligns social structure and marginalization of social science principles to ensure that a policy is fair for all.

Career Connection to Society

While cybersecurity policy analysts affect many organizations and individual users, policy analysts also affect societal resilience, trust is digital systems, and civic equality. A policy analyst ensures that marginalized communities are not excluded from digital safety, they contribute to social justice, equality, and inclusive security for all groups. Their work helps ensure that every organization and individual, even those who don't have access to the internet is benefited from new policies rather than just the people who use the internet every day.

Conclusion

A cybersecurity policy analyst perfectly shows how cybersecurity is about much more than technology, hardware, and software. It is about people, organizations, societies, governments, and the behavior of people and hackers. By using social sciences principles like psychology, sociology, and political science in their everyday routine, these analysts can shape new policies that are effective, and socially inclusive for all. Concepts like relativism and empiricism that we discussed in class play a large role in this job as well. Policy analysts make new policies with marginalized groups in mind and that is why they can uphold their main mission and that is digital security for all. Organizations and Governments applying policy analysts who understand and apply social science principles to their work can be the difference between a safe digital environment for everyone and chaos for marginalized groups and society as a whole.

Scholarly Journal Articles

CloudDefense.Ai. (2023). Importance of Cyber Security Policy. In *Medium*. https://medium.com/@clouddefenseai/importance-of-cyber-security-policy-7ad8446b09a8

Board, C. S. a. T., Sciences, D. O. E. a. P., & Medicine, N. a. O. S. E. A. (2017). Foundational Cybersecurity research. In *National Academies Press eBooks*. https://doi.org/10.17226/24676

{"@type": “Person”,"name": “Aubra Anthony”}. (n.d.). *Cyber resilience must focus on marginalized individuals, not just institutions*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/03/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions?lang=en