Cybersecurity Professional Career Paper: Cybersecurity Policy Analyst

Student Name: Dmitriy Yeremin

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 03/20/2026

Introduction

My chosen career for this paper is policy analysts. This career sits at the intersection of software engineers and top tier government bodies. Policy analysts must understand cybersecurity fundamentals and procedures, but they are not expected to be engineers. Cybersecurity is growing in importance due to the rapid digitalization of society. Many companies and organizations are automating key procedures within their business which creates new threat vectors. Also, more people are getting exposed to new digital systems and lack the knowledge of operating and securing them properly. The purpose of this paper is to connect my chosen career to social science principles, concepts, and express the importance of policy analysts.

Social Science Principles

Policymakers and analysts would not be very effective without the support of social sciences to guide their frameworks. Social sciences help them understand why people do what they do and within specific settings, an experiment can take place to study these decisions more in depth. Parsimony is a principle that is used to better communicate standards and frameworks to all different kinds of employees. Not everyone is tech savvy, so because of that policy analysts need to communicate their points in a clear and simple way. Another principle that is prevalent in this career is determinism. Policies are made because of certain actions or events from the past or foreseeable future. Another side to determinism is the behavior of employees being caused by the actions of the policymakers. Professionals have used behavioral psychology to understand the impact and influence of cybersecurity training. “The protection motivation theory (PMT) was employed to understand the behavioral change after the implementation of cybersecurity

training… the PMT based training was effective in increasing the threat knowledge of the students along with the increase in information of countermeasure strategies (Khan et al., 2023)". Policy analysts have a direct connection to the trainings that take place within their organizations. Many social science insights like behavioral psychology and objectivity allow professionals to review factual conclusions about individuals' behavior around digital safety.

Application of Key Concepts

Policy analysts are a great example of a career field where our class concepts appear frequently. Many analysts perform multiple reviews of current policies to make sure they are up to date with standards set by higher organizations like IEEE and in line with the company's mission. This is done through objective reviews of incident response briefings. Analysts will break down the reported actions of individuals to ensure they acted within accordance to frameworks. Reviewing archival material and case studies such as past logs and debriefings allow policy analysts to assess the compliance of security protocols and legal standards. Another concept from class that is used in this field is multi-method research which can be used in the form of comparative research. Assessing how competitors or very successful companies with similar goals implement policies and standards is a common way of practicing self-awareness as an organization. All current and new policies will have the CIA triad in mind when implemented. Additionally, the NICE framework is critical for providing a structured methodology for defining roles, responsibilities, and required competencies of cybersecurity professionals, which policy analysts use to ensure their workforce standards align with national guidelines.

Marginalization

Marginalization is a topic that comes up more frequently in cybersecurity policy discussions. Some communities have less access to updated technology and lack knowledge in digital education, which can leave them more vulnerable to cyber threats. Policy analysts must keep this in mind when creating frameworks because a policy that works for a large corporation or one category of a population might not work the same way for everyone else. Part of the job is making sure the policies being written cover all groups of people effectively.

In the workforce domain, there have been pushes to bring more diversity into the cybersecurity field. The NICE framework helps policymakers with this by providing guidance on workforce development and inclusive hiring methods. Policy analysts use these standards to help organizations build teams with a wider range of perspectives which leads to better and more applicable security policies. Research has shown that incorporating social science principles into cybersecurity education can better prepare professionals and help close gaps between academic training and real-world application (Khan et al., 2023).

Career Connection to Society

One of the benefits of having organizations like IEEE or NIST is that policy analysts, in all different career fields, can implement their standards and policies. They are not bound to a specific field. There might be some additional policies required for medical fields or other specialized sectors, but they can easily be integrated into existing frameworks. Without proper cybersecurity frameworks in place, critical sectors like healthcare and financial institutions become vulnerable to attacks that can have devastating consequences for ordinary people. To give an example of a public policy and its implications: The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires covered entities to report covered cyber incidents and ransomware payments to CISA; This will allow CISA to quickly deploy resources

and give assistance to victims, additionally this will give CISA the opportunity to spot trends and share this critical information to other network defenders (CISA, 2022). I see this public policy as an opportunity to lift some of the burden off of the organizations so that CISA can do the heavy lifting and provide relief.

Scholarly Journal Articles

The first source is communicating the findings of Khan et al. (2023). The study evaluated cybersecurity awareness training utilizing Protection Motivation Theory and found that PMT training effectively increased participants' threat knowledge and understanding of countermeasures. This directly supports the paper's discussion of how behavioral psychology is used by professionals to design more effective cybersecurity training programs. The second source, Maalem Lahcen et al. (2020), supports the social science principles by demonstrating that professionals draw on psychology, sociology, and behavioral economics. They use these disciplines to develop awareness campaigns and user training programs that account for human factors. It reinforces the argument that cybersecurity is not just a technological issue, but a human centered dilemma. The third and final source, CISA (2022), deepens the understanding of career connections to society by providing a real-world example of public policy. Policymakers have a great opportunity to help the public by taking on the burden of threat response and escalating incidents to agencies with greater authority and resources.

Conclusion

This paper captured the essential responsibilities of a policy analyst. Social science principles and concepts were observed and explained to fully bridge the relationship between them and the career. Policy analysts are not just concerned with the technological side of

cybersecurity. They take human factors into serious consideration when building new policies for institutions or for the public. The career of a policy analyst has a major impact on the organizations and communities they serve. The future of companies relies on the progress of policymakers and without effective policy guidance organizations are left vulnerable and directionless.

References:

Cybersecurity and Infrastructure Security Agency. (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*. U.S. Department of Homeland Security. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, *125*, 103049. https://doi.org/10.1016/j.cose.2022.103049

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00050-w