Cybersecurity Professional Career Paper: Cyber Policy and Strategy Planner

Kirstie Joseph

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

May 7th 2026

Introduction

The career I would like to pursue in cybersecurity is that of a Cyber Policy and Strategy Planner. This is a cybersecurity professional whose role is responsible for developing policies, strategies, and long-term security plans that support the goals of an organization and regulatory compliance. According to the Cybersecurity and Infrastructure Security Agency, professionals in this role help organizations align cybersecurity initiatives with laws, risk management practices, and national security objectives (CISA, n.d.). In our modern society, cybersecurity is critical to everything. Governments, healthcare systems, financial institutions, and businesses all depend on technology and interconnected networks. Cyberattacks can disrupt essential services, expose highly sensitive data, and jeopardize national security. This paper will analyze how social science principles connect to the role of a Cyber Policy and Strategy Planner, how fundamental cybersecurity concepts are applied within the profession, the impact this field has on marginalized groups, and how these professionals positively contribute to society through policy development and strategic cybersecurity planning.

Social Science Principles

Cyber Policy and Strategy Planners rely heavily on social science principles because cybersecurity problems are often caused by human behavior, not just technology. Human error, phishing, insider threats, social engineering, and poor security practices all display how social science influences cybersecurity risks. Professionals who hold this position study how people interact with systems, respond to policies, and make security decisions. For example, research based in social science helps cybersecurity professionals understand why employees tend to ignore security protocols and fall for phishing attacks. Cyber Policy and Strategy Planners use

this data to create policies and awareness initiatives that promote safe online behavior. Instead of only focusing on technical solutions, they lead by considering communication styles, business culture, ethics, and human decision-making. This role balances cybersecurity with privacy rights, ethical concerns, and the trust of the public (CISA, n.d.).

Social science principles are integrated into human-computer interaction and are concepts that are constantly considered within this profession. A system being "user-friendly" is extremely important because if security systems are too complicated, users may find ways to ignore or bypass them entirely, putting themselves at risk for the sake of convenience. Policy planners develop strategies that are not only secure but practical for real-world users while also communicating to stakeholders why these policies need to be followed.

Application of Key Concepts

Similar to most, if not all, roles in cybersecurity, one of the major cybersecurity concepts related to this career is the CIA Triad: confidentiality, integrity, and availability. Cyber Policy and Strategy Planners help organizations protect confidentiality by creating data privacy policies and access control standards. They support integrity by implementing procedures that prevent unauthorized changes to user information. They maintain availability by developing incident response plans and continuity strategies to reduce downtime during cyberattacks.

Compliance and governance, which are my main interests, are also important responsibilities in this role. Cyber Policy and Strategy Planners help organizations follow cybersecurity laws, regulations, and frameworks such as the NIST Cybersecurity Framework.

Their duties may include conducting risk assessments, developing incident response plans, and creating security policies that support organizational goals.

Marginalization

Cybersecurity may affect marginalized groups differently because of unequal access to cybersecurity education and resources. Unfortunately, these groups often become targets for scams, fraud, and identity theft due to these disadvantages. Healthcare and financial information exposed through data breaches can inflict even greater harm on people already facing socioeconomic disadvantages.

Cyber Policy and Strategy Planners aim to address these circumstances by developing policies that support privacy, fairness, and digital protection for all users. This type of work helps combat discrimination, improve data protection, and ensure cybersecurity policies are applied ethically.

Career Connection to Society

Cyber Policy and Strategy Planners contribute to the safety and stability of societal infrastructure such as hospitals, banks, transportation systems, critical infrastructure, and government networks by helping organizations prepare for cyber threats and reduce risks to public safety through the development and enforcement of cybersecurity policies and strategic defense protocols. This career also connects strongly to public policy because cybersecurity laws and regulations influence how organizations collect, store, and protect personal information, which ultimately improves cybersecurity practices.

Scholarly Journal Articles

Cyber Defense as a Complex Adaptive System: A Model-Based Approach to Strategic Policy Design explains that cybersecurity requires adaptive policy design and strategic planning in order to succeed in responding to evolving cyber threats. This is relevant to Cyber Policy and Strategy Planners because it focuses on governance, risk management, and organizational cybersecurity strategy (Norman & Koehler, 2017).

Cybersecurity professionals must understand why people ignore security practices or fall victim to cyberattacks. *Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?* supports how human behavior and psychology influence cybersecurity awareness and policy compliance (Bada et al., 2015).

Savaş and Karataş (2022) explain in *Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance* how cyber governance helps organizations manage risk, maintain compliance, and protect critical infrastructure. This contributes to understanding how Cyber Policy and Strategy Planners use governance and policy to support both organizations and society.

References

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). *Cyber security awareness campaigns: Why do they fail to change behaviour?* Oxford University Global Cyber Security Capacity Centre.

https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8/files/ma93418816f0d35c131edbdd0b13cea13

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cyber policy and strategy planner*. U.S. Department of Homeland Security.

https://www.cisa.gov/careers/work-rolescyber-policy-and-strategy-planner

Norman, M. D., & Koehler, M. T. K. (2017). *Cyber defense as a complex adaptive system: A model-based approach to strategic policy design*. arXiv. https://arxiv.org/pdf/1706.08598

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 3*, 7–34.

https://pmc.ncbi.nlm.nih.gov/articles/PMC8750646/