**The Role of Social Science in Cyber Policy and Strategic Planning**

Dominique Rhodes

Cyber Security and Social Science

Teresa Duvall

**Introduction**

Today, we live in the digital age, and with that comes the ever-evolving field of cybersecurity. Professionals whose career focus is cyber policy and strategic planning are on the front lines of cyber defense, working to safeguard nations, organizations, and individuals from cyber threats. Although technical expertise is vital to this role, social science research and principles are just as important. This paper will highlight the relation and significance of social science in cyber policy and strategic planning, demonstrate its application in daily duties, and explore its effects on society by utilizing the concepts learned in my Cybersecurity as a Social Science class.

**Cybersecurity as a Social Science**

In class, we learned that “Robert Bierstedt (1970) argued that the social sciences adhere to the same principles as the natural sciences.” (Duvall, 2023) These principles are relativism, objectivity, determinism, ethical neutrality, skepticism, and parsimony. Right off the bat, relativism speaks to the relation of all things. This can be attributed to cybersecurity due to the interwoven connection of all systems, including social media, health care, education, critical infrastructure, politics, criminal justice, and technical systems. (Duvall, 2023) With that being said, let’s explore how this relates to the role of cyber policy and strategy planning.

**The Role**

The NICE framework defines a cyber policy and strategy planner as someone who develops and maintains cybersecurity plans, strategies, and policies to support and align with organizational cybersecurity initiatives and regulatory compliance. (Strategic Planning and Policy, n.d.)

As stated earlier, cyber policy and strategy planners spearhead nations, organizations, and individuals. What do these three have in common? The answer is people. These plans and strategies are put in place for the protection of people. To better these plans and strategies, planners must be able to research and understand human behavior and behavioral sciences, which are key components of social science. For example, crowd strike lists phishing as the third most common attack. Phishing attacks lead to data breaches, which on average cost 4.45 million dollars, a 15% increase over three years. Also, 51 percent of organizations are planning to increase security investments. Cyber policy and strategy planners are paid to create the policies and plan for testing, training, threat detection, and threat response to mitigate costly breaches. This doesn’t just affect businesses. In 2022, phishing statistics show that in 2022, there were 300,497 phishing victims, with a total loss of $52,089,159 in the U.S. alone. (Main, 2023) To combat this, planners work daily to develop user training plans, strategies, and compliance initiatives. These plans and strategies are driven by data and research that explore why employees fall victim to these attacks.

**Closing the Margin**

In 2023, a new White House national cyber strategy was released. It is the first comprehensive cyber plan released by the White House since 2018. Its goal is to shift from a reactive to a proactive approach to a cybersecurity posture and push more accountability in the tech industry. There are two challenges that I expect to affect marginalized people. The first is one the government and I both agree on, and that’s the challenge of an inferior cybersecurity workforce. The white house recognizes an issue with the cyber security workforce, possibly due to the lack of diversity. Online recruiter Zippia estimates that in 2021, around 91% of chief information security officers are men, and nearly 65% are white. (Riotta & Alms, 2023) Another challenge will be the challenge of expanding these strategies and plans to everyday people. The plans, strategies, and initiatives mainly focus on the institutions, organizations, and government. Cybercriminals exploit low-income people with little digital literacy. With inflation and the current state of the economy, why would a person invest in software like McAfee to protect their devices when living paycheck to paycheck? So, as a cyber policy and strategy planner, how can you work for the common folk as well as the banks, big companies, and government to better secure cyberspace as a whole?

**Conclusion**

In conclusion, the role of cyber policy and strategy planners is undeniably crucial to our modern society. These professionals act as the guardians of our digital realm, working tirelessly to protect nations, organizations, and individuals from the ever-growing threats in the cyber landscape. However, their effectiveness doesn't solely rely on technical expertise but on their understanding of social science principles. Even under the capability indication tab in the NICE Framework, certification examples include certifications/credentials that use principles of psychology, which is also a branch of social science, to implement policy. With this, planners can develop more effective policies and strategies that safeguard businesses and benefit civilization by bridging the gap between technology and human behavior.

REFERENCES

*2023 global threat report: CrowdStrike*. crowdstrike.com. (2023, July 13). https://www.crowdstrike.com/global-threat-report/?CT-2023-Q1-cyber101heroB-attacktypes-GTR-CTA

*Cost of a data breach 2023*. IBM. (n.d.). https://www.ibm.com/reports/data-breach

Main, K. (2023, July 17). *Phishing statistics by state in 2023*. Forbes. https://www.forbes.com/advisor/business/phishing-statistics/

*Read “A decadal survey of the social and behavioral sciences: A research agenda for advancing intelligence analysis” at nap.edu*. 6 Integrating Social and Behavioral Sciences (SBS) Research to Enhance Security in Cyberspace | A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis | The National Academies Press. (n.d.). https://nap.nationalacademies.org/read/25335/chapter/10

Riotta, C., & Alms, N. (2023, July 10). *National Cyber Strategy faces major implementation challenges, experts say*. Nextgov.com. https://www.nextgov.com/cybersecurity/2023/03/national-cyber-strategy-faces-major-implementation-challenges-experts-say/383561/

*Strategic planning and policy*. National Initiative for Cybersecurity Careers and Studies. (n.d.). https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/strategic-planning-and-policy

*Duvall, T. (2023). CYSE201S Module 2 Fall 2023 [PowerPoint slides]. Department Name, Old Dominion University. https://canvas.odu.edu/courses/140948/files/25905984/download?download\_frd=1*

*Duvall, T. (2023). CYSE201S Module 2 Fall 2023 [PowerPoint slides]. Department Name, Old Dominion University. https://canvas.odu.edu/courses/140948/files/25905984/download?download\_frd=1*