Analysis of The National Cybersecurity Strategy of the United States

Brandon Zachary Pearson

Old Dominion University

CYSE425W - CYBER STRATEGY AND POLICY

Professor Malik A. Gladden

December 4, 2023

The National Cybersecurity Strategy of The United States is a comprehensive attempt at addressing areas that lack fortification when it comes to cybersecurity. With the rise in cyberattacks and breaches occurring in recent years, it is a better time than ever. Technology gets more advanced every year and often cybersecurity developments are falling behind. The United States is attempting to remedy this by attacking the issue in a collaborative manner. This means the strategy is heavily reliant on the collaboration of multiple different sectors and entities. This results in this strategy having major social implications on society.

One of the major reasons this strategy has come about is due to the internet's social impact across the world. The Internet is deemed a critical infrastructure due to the massive impact it has on various social aspects in the United States. Without the Internet, many important tasks wouldn't be able to be completed. In addition, many infrastructures in society require the internet and in the event of an attack could destroy various functions that are needed for society to function orderly. Aside from this, the internet has allowed everyone to become more interconnected. Having internet access and using devices that require internet access are at an all-time high. This only makes cyberattacks more likely due to the increase in devices connected to the Internet. With each new digital device or IoT device created it only increases the likelihood of an attack could occur. "However, many of the IoT devices deployed today are not sufficiently protected against cybersecurity threats. Too often they have been deployed with inadequate default settings, can be difficult or impossible to patch or upgrade, or come equipped with advanced—and sometimes unnecessary—capabilities that enable malicious cyber activities on critical physical and digital systems" (NCSS, p.20). This dependence on internet-connected devices within the nation could leave individuals in a state of panic if an attack occurs. This isn't made any better when many IoT devices don't have great cybersecurity features implemented.

Another concern with the interconnectedness of the internet is the amount of data that is being transmitted. This poses a great risk because a cyberattack can have more than just social impacts.

This strategy emphasizes the importance of collaboration in order to achieve the goal of creating a more secure cyberspace. This collaboration impacts social factors between the different entities in society. This is necessary because one entity can't create a safer cyberspace. It will take each entity to do its part to contribute to the bigger picture. The government, corporations, and individuals each have responsibilities that will decrease the likelihood of an attack.

The government putting in place regulations and policies that oversee corporations to ensure that they are implementing proper cybersecurity features. Additionally, requiring implementation will undoubtedly create an uncomfortable environment between corporations and the government. While the goal the government wants to reach is great many corporations will likely be opposed to adding additional regulation and polices to their sector. Corporations could feel that additional government involvement in their sector restricts them from pursuing things they would like. "One side of the debate about government involvement holds that the private sector has not adequately implemented measures to protect themselves against cyber threats, warranting government involvement" (Lino). At the same time, it requires companies to spend large sums of money on things they didn't initially want to.

This strategy also impacts individuals in society because it could restrict the things, they have access to. This strategy may bother individuals who feel as if the things the government is attempting to implement in order to reach their goal could be unethical. It is common that the public doesn't like the government having too much involvement in their lives. "Policymakers must consider a range of factors, such as political feasibility, economic impact, and social

acceptability, when creating policies" (Walker). One other thing that this strategy is wanting to do is provide more education and resources for individuals to have access to. This is a good thing and could teach individuals how to be safer when it comes to managing computer hygiene. The government has to ensure there is a balance between what society wants and is okay with and what the government wants.

This strategy has various social impacts within society. When implementing this strategy, it will undoubtedly shift the culture surrounding cybersecurity and the importance of it, seeking a level of collaboration amongst the government, corporations, and individuals to help the nation defend itself. Introducing concerns around regulations and policies that may restrict the nation in various ways. Disrupting how society functions and what is important going forward.

Works Cited

Lino, Christine. “Cybersecurity in the Federal Government: Failing to Maintain a Secure Cyber Infrastructure.” Bulletin of the Association for Information Science & Technology, vol. 41, no. 1, Oct. 2014, pp. 24–28. EBSCOhost, https://doi-org.proxy.lib.odu.edu/10.1002/bult.2014.1720410111.

National Cyber Workforce and Education Strategy - the White House, www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

Walker, Smith. “The Importance of Public Policy in Shaping Society.” Journal of Public Health Policy and Planning, Allied Academies, www.alliedacademies.org/articles/the-importance-of-public-policy-in-shaping-society-24022.htm