Political Impact of the National Cybersecurity Strategy of the United States

Brandon Zachary Pearson

Old Dominion University

CYSE425W - CYBER STRATEGY AND POLICY

Professor Malik A. Gladden

September 29, 2023

Cybersecurity has become one of the most important things to improve on in recent years. Cyber attacks are becoming more advanced and more frequent each and every day. This concern with cyberattacks has become so prevalent that the United States developed the National Cybersecurity Strategy. The National Cybersecurity Strategy of the United States was last updated in March of 2023. The major focus of this update was "The National Cybersecurity Strategy calls for two fundamental shifts: rebalancing the responsibility to defend cyberspace and realigning incentives to favor long-term investments." (U.S. Department of State. 2023, March 8). With any new policy, there are political implications as well as ramifications that arise. Reviewing the steps that policymakers are taking in order to resolve any issues that have come about. As well as understanding the viewpoints of policymakers in order to understand the reasoning behind the implementation of The National Cybersecurity Strategy.

The United States strives to upgrade the policies surrounding cybersecurity due to the frequent cyber attacks. As the internet and IoT devices expand more security concerns arise. This is due to the rapid development of new devices which only allows attackers to capitalize on the lack of security features. "In a survey of 582 information security professionals, 50% say they do not believe their organization is prepared to repel a ransomware attack." (Jason Firch, M.). Ransome attacks are one of the most costly types of attacks and can greatly hamper the organization that was attacked. These are just one of the major concerns when it comes to cyberattacks. The U.S. wants to create a safer cyber environment in order to prevent attacks from committing attacks on any form of critical infrastructure. Critical infrastructure can be anything from gas, electricity, transportation, and other things that keep the United States interconnected. Another major concern that leads politicians to address this issue in the U.S. is the economic impact cyberattacks can have on citizens. Attacks can put their private data at risk for exploitation or disrupt the daily lives of U.S. citizens. In recent years cyberattacks have become prevalent enough that most people know what they are and the risk they pose. This has created an environment where the government must address the issues at hand.

Some of the politicians who have pushed for the development of the National Cybersecurity Strategy are President Biden, Kamala Harris, Jen Easterly, and Ron Wyden. Biden enacted Executive Order 14028 which enforced that stronger cybersecurity efforts be put in place. Highlighting that encryption should be utilized as well as the NIST framework be implemented in government organizations. Additionally, Biden issued the National Security Memorandum 5 which targets critical infrastructure (The United States Government. 2021, July 28). Creating more policies that attempt to place guidelines with the goal of reducing the likelihood that an attack can take place.

Jen Easterly holds the position of the United States Director of the Cybersecurity and Infrastructure Security Agency. In this role, she is set out with the task of ensuring the security of the United States. While Easterly has been in this role she has pressed for the importance of the CISA. That it is needed in order to ensure that the nation and government are putting their best efforts into defending the U.S. In 2018, Easterly as well as former President Donald Trump helped establish the Cybersecurity and Infrastructure Security Agency Act. This act placed stricter policies and guidelines for certain sectors of the government.

Ron Wyden a U.S. senator for Oregon, has been a big supporter of implementing stronger legislation in place for cyber security. Primarily target data privacy and user rights. Wyden has also wanted to keep a balance between governmental involvement in users' information and privacy. Wanting to have a more transparent government in order to prevent the government from overstepping human rights.

The National Cybersecurity Strategy hasn’t been met with complete open arms. One of the major complications is the need for corporations between the government sectors and corporations. One of the reasons for this is the lack of knowledgeable cybersecurity professionals on both sides. Additionally, the cost of implementing more secure cyber defenses can be high which makes corporations slow to come around. With the government becoming more evolved with cybersecurity it has also introduced concerns with the extent government will go to ensure a secure cyberspace. The balance between creating a more secure government can come at the cost of the public's right to privacy. One major ramification that has come about with the development of stronger policies is that it has put the government-involved sectors under more security. This can be by the public or by other government sectors if breaches happen or if it is revealed that there has been little effort put forth to meet guidelines.

The major complication that the United States government has when it comes to creating a safer cyberspace. Comes down to that it has to be done without overstepping or encroaching on the public's civil rights. This is a complicated process due to the need for cyber defense in this day and age. In recent years, there have been many improvements in cybersecurity, but it has been slow in implementation due to various reasons. This is why there is a need for governmental involvement when it comes to ensuring the country's security.

References

Cisa Cybersecurity Strategic Plan: Shifting the arc of national risk to create a safer future: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2023, September 29). https://www.cisa.gov/news-events/news/cisa-cybersecurity-strategic-plan-shifting-arc-national-risk-create-safer-future#:~:text=The%20National%20Cybersecurity%20Strategy%20sets,Cybersecurity%20Strategic%20Plan%20comes%20in.

Jason Firch, M. (2022, November 11). 10 cyber security trends you can't ignore in 2021. PurpleSec. https://purplesec.us/cyber-security-trends-2021/

Kelley, A. (2023, July 10). Report spotlights medical infrastructure, utilities as primary cyber targets. Nextgov.com. https://www.nextgov.com/cybersecurity/2023/03/report-spotlights-medical-infrastructure-utilities-primary-cyber-targets/383543/

National Archives and Records Administration. (n.d.). The Comprehensive National Cybersecurity initiative. National Archives and Records Administration. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

Office, U. S. G. A. (n.d.). Cybersecurity: Launching and implementing the National

Cybersecurity Strategy. Cybersecurity: Launching and Implementing the National Cybersecurity Strategy | U.S. GAO. https://www.gao.gov/products/gao-23-106826#:~:text=In%20March%202023%2C%20the%20White,to%20drive%20security%20and%20resilience

U.S. Department of State. (2023, March 8). Announcing the release of the administration's National Cybersecurity Strategy - United States Department of State. U.S. Department of State. https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/

The United States Government. (2021, July 28). National security memorandum on improving cybersecurity for Critical Infrastructure Control Systems. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

The United States Government. (2023, March 2). Fact sheet: Biden-Harris Administration Announces national cybersecurity strategy. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/#:~:text=The%20Administration%20has%20already%20taken,%2D22%2D09%20(Moving%20the