Introduction

The National Cybersecurity Strategy is an extensive policy created to address the rising concern of cyber attacks on the United States federal government. In today's day and age, the implementation of such a plan is more important than ever. As the government continues to witness cyber attacks taking their toll on the economy each year, they can no longer brush it off as a personal issue that people and businesses have to take into consideration and has now become a national subject. In today's society the Internet of Things(IOT) has changed the way our society operates, as we as a civilization have become more and more dependent on technology's advances, we have also made ourselves more vulnerable then ever to cyber attacks. 66% of North American homes contain at least one IoT device, most of these devices contain some type of personally identifiable information (PII) saved on them, leaving those who own said devices susceptible to having their information compromised in a cyberattack. As such the National Cybersecurity Agency developed the National Cybersecurity Strategy, claiming, "This strategy will position the United States and its allies and partners to build that digital ecosystem together, making it more easily and inherently defensible, resilient, and aligned with our values. By the end of this decisive decade, we will achieve these outcomes so we can confidently take bold leaps into a digitally-enabled future that benefits us all."

Breakdown

The strategy consists of five pillars to defend against cyber attacks, "Defending Critical Infrastructure", "Disrupt and Dismantle Threat Actors", "Shaping Market Forces", "Investing in a Resilient Future" and "Forging International Partnerships". To better understand the overall purpose, it is important to understand the meaning of each pillar. The first pillar can be summed up as minimizing the possibility of essential national services being corrupted. The second pillar focuses on developing a counter attack strategy for cyber attacks. The third pillar encourages organizations in the country to put more emphasis on security by shaping market forces. The fourth pillar promotes the investment in the continuous development of cybersecurity innovation to make the future outlook in the security field better. Finally the fifth pillar works to forge partnerships with other nations to strengthen cybersecurity cooperation internationally.

Effectiveness

The strategy, if implemented correctly, can be very effective at building the nation's cybersecurity infrastructure. The strategy is extremely thorough and its five pillars focus on different aspects of advancement needed in cybersecurity. Not only does it highlight important concepts such as defending the nation's critical infrastructure, an issue that has been prevalent in the past, but also looks to improve upon past mistakes and create a better future, highlighted through pillar's four and five.

The issue with the strategy however, is the concept of its implementation. Taking example from the popular NIST cybersecurity framework for example, an organization can spend anywhere from 35,000-100,000 dollars if they are correctly complying with NIST regulations. (Cost of Compliance), it can be expected that a strategy is implemented on a national level, this can also make it especially difficult for organizations across the country to comply. To combat this the federal government is taking a "data driven" approach to the implementation, "measuring investments made, progress, and effectiveness of these efforts." (Unpacking the White House National Cybersecurity Strategy).

Pillar one: Defending Critical Infrastructure

Defending Critical Infrastructure is one of the most important pillars throughout the strategy. Critical Infrastructure has been the target of multiple cyberterrorism attacks on the country, so it is quite fitting that a national strategy would address this issue. This pillar has five strategic objectives, Establish Cybersecurity Requirements to Support National Security and public safety, Scale Public-Private Collaboration, Integrate Federal Cybersecurity Centers, Update Federal Incident Response Plan, and Modernize Federal Defenses.

The first objective addresses the issue that owners of critical infrastructure that invest in cybersecurity related practices. The strategy attacks this issue by claiming that regulations can help to level the playing field. The strategy aims to require tailored frameworks for each industry, with the frameworks changing depending on the sector's risk profile. While this tactic may be costly, it enforces these industries to adhere to standards to "meet the needs of national security and public safety".

The second objective of the pillar aims to promote the collaboration of the public and private sectors to increase the overall security hygiene in the nation. The Cybersecurity and Infrastructure Security Agency(CISA) is designated as the national coordinator for critical infrastructure security and resilience. The strategy outlines that "CISA coordinates with Sector Risk Management Agencies (SRMAs) to enable the Federal Government to scale its coordination with critical infrastructure owners and operators across the United States.". This tactic allows for close relations with critical infrastructure operators to work with national organizations to ensure that they are not only adhering to national standards but also helps to better improve cybersecurity practices.

Objective number four promotes the modernization of federal incident response plans. The plan states that CISA will lead a process to update the National Cybersecurity Incident Response Plan (NCIRP). This is one of the simpler additions to the infrastructure that still has a key effect on security hygiene. Keeping the federal response plan up to date consistently allows for the best possible response to always be concrete and available. Because of cybersecurity's lack of prevalence in recent years it can be easy to be overlooked if not set as a standard for it be revised.

Conclusion

Overall, pillar one allows for the prioritization of critical infrastructure in the National Cybersecurity Strategy. It is a prime example of how the strategy aims to look at past mishaps in the cybersecurity community to create a more security-driven future. The pillar also takes a risk-based approach, allowing organizations to allocate resources properly and effectively. While the approach can be costly for organizations new to allocating resources for cybersecurity, it is important to ensure that these organizations are required to properly put cybersecurity practice as a priority. This practice also makes the strategy as a whole more effective in addressing growing needs in today's society. The National Cybersecurity Strategy as a whole provides a solid framework through which the country can learn from. Although it's implementation still provides a challenge, through consistent work it can improve the overall cybersecurity hygiene of the country and open the doorway for a more secure future for citizens of the country.

Works Cited

Cost of Compliance | CMMC and NIST 171 | Hyper Vigilance. (n.d.). Blog.hypervigilance.com. Retrieved February 26, 2024, from https://blog.hypervigilance.com/cost-of-cmmc-nist-compliance#:~:text=Under%20these%20assumptions%2C%20an%20organization

National Cybersecurity Strategy--Going Where No Strategy Has Gone Before (IN12123) [2023]. (2023).

National Cybersecurity Strategy: Key Improvements Are Needed To Strengthen The Nation's Posture. (2009).

Unpacking the White House National Cybersecurity Strategy: Hearing Before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation of the Committee on Oversight and Accountability, House of Representatives, One Hundred Eightee. (2023). U.S. Government Publishing Office.