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

November 1, 2023

Cyberspace has changed rapidly over the last three decades. At the start of the internet, it wasn’t designed with the thought that it would be as massive as it is today. This has led to many issues arising over time. One of the major areas that was underdeveloped and lacking through forethought was the security features of the internet. Due to this, security aspects have been a major area that needs improvement to ensure a safer cyberspace. The United States has noticed the lack of pre-established cyber security measures regarding the internet. Which has led to the creation of The National Cybersecurity Strategy of the United States. This policy was established in March of 2023 to address the growing threat to the United States’ digital ecosystem. The main goal of this policy is to relieve the burden of cybersecurity from the public by putting more effort into government organizations that can ensure a safer cyberspace at a fundamental level. This would allow the government to ensure a safer cyberspace for the U.S. by taking charge of the cybersecurity plan going forward rather than leaving it up to the public to prioritize their own safety.

The National Cybersecurity Strategy of the United States is broken down into five major “pillars” all having a different focus and perspective on how to achieve a safer digital ecosystem. The five pillars are: Defending Critical Infrastructure, Disrupting and Dismantling Threat Actors, Shaping Market Forces to Drive Security and Resilience, Investing in a Resilient Future, and Forging International Partnerships to Pursue Shared Goals. Each of the pillars goes over and recognizes the level of importance each pillar has in defending the U.S. from cyber attacks. “Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences.” (National Cyber Workforce and Education, 2023). The strategy hopes to create a space where the U.S. and its allies can work together to develop cyber defense policies and tactics further. The rise of malicious actors and cyberattacks within the last generation has caused rapid concern for such collaboration. The internet has become something that is ingrained into society to the point that it has become essential and by most considered a critical infrastructure. Further adding to the concern that future cyberattacks could have drastic effects on U.S. citizens by impacting critical infrastructure. Additionally, many essential systems of society have become digital and rely heavily on a secure cyberspace. Only making the U.S. push to create a cybersecurity strategy that could address the worries of the potential damage that can be done via cyberspace.

The strategy seeks to defend critical infrastructure by collaborating with private sectors to ensure that they are working together to ensure that long-term investments into cybersecurity are taking place. While keeping a long-term goal in mind, they want also to manage the systems that are around now to keep them safe from malicious actors. The collaboration between states and the government is a hard task to accomplish. While it is important to create a safer cyberspace it can be a hard task to get corporations involved. It is one of their social responsibilities as a business to protect their users, but businesses want to be profitable. This can make it hard to get corporations behind corporations with the government since it could lead to them having to spend large sums of money. The government understands this and will focus on creating some form of incentive to gain cooperation between the two. “To achieve these goals, the Federal Government will focus on points of leverage, where minimally invasive actions will produce the greatest gains in defensibility and systemic resilience” (National Cyber Workforce and Education, 2023). Many companies specialize in cybersecurity and have other crucial resources that will be needed in order to accomplish this task. Therefore, the private sector needs to do its part to offer more resources to the cause.

The National Cybersecurity Strategy of 2023 is the United States' way of taking a more proactive approach to combating cyber threats. Notable cyberattacks such as the Colonial pipeline attack, Equifax breach, and SolarWinds breach have been key points for the development of this strategy. The SolarWinds attack was a great example of how a single company being breached can lead to multiple companies being breached. Even more pressing is that many government agencies were breached due to the SolarWinds breach. Now more than ever is the time for this strategy to take effect in order to prevent such attacks.

The National Cybersecurity Strategy sets out to accomplish many things with each pillar. The one pillar with the most importance is the first pillar “Defending Critical Infrastructure”. The other four pillars stem from this pillar and are the actions that will defend critical infrastructure. When it comes to cyberattacks one of the most concerning types of attacks are ones that target critical infrastructure. Targeting critical infrastructure has the capability to destabilize countries or regions. Another issue that comes with protecting critical infrastructure is that many different sectors are deemed to be critical. This makes creating policies hard because not all sectors are the same. Each sector will have to have its own set of policies to ensure that they are doing what it can to defend that particular sector. Similar to how rules and regulations have to be altered depending on the type of sector it is being applied.

This strategy sets out to accomplish this goal by requiring sectors to abide by set regulations and policies when it comes to cybersecurity. This is in hopes that creating more strict rules around cybersecurity will lead to companies being less likely to be breached. In addition to this, the government and government agencies are going to work to strengthen their defense. If both government agencies and corporations start to develop cybersecurity features, it can mutually benefit each other. Both the corporations and the government can aid each other in ensuring that critical infrastructure is being managed properly.

The United States is also switching to a zero-trust architecture strategy when it comes to infrastructure. This concept is that every device should not be trusted and can always be someone attempting to commit malicious acts. This strategy further goes on to that each device must be verified before it is trusted. “The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access.” (Office of Management and Budget, 2022).

Creating an overall more secure network because devices won’t have access unless they are verified to be a trusted user. Furthering this, even devices that are trusted should be viewed and verified to ensure they haven’t been compromised. This can help prevent attacks that are taking place and prevent attackers from furthering an attack.

One major thing that also is being addressed is the federal incident response plans. This is being developed in order to offer solutions and assistance from the government if corporations are under attack. Giving corporations an easy way to contact government agencies in order to receive help. This is important because the earlier government agencies can get involved the less damage can be done by attackers. Additionally, this gives agencies the ability to analyze what happened during the attack to determine what may have been targeted. Essentially it allows them to do digital forensics more effectively by allowing them to respond faster to incidents that take place.

Another thing that is being done is to centralize government agencies around one integral cybersecurity center. This sets up an easier way to distribute ideas, and solutions, and communicate. This collaboration can allow for a more streamlined way to share information that could potentially be vital. Particularly making sure that human-to-human communication is emphasized. This can also improve user awareness lessening the likelihood that social engineering takes place.

Overall, the National Cybersecurity Strategy is an important policy that sets out to accomplish a large task. Attempting to create a safer cyberspace by implementing new regulations and policies across the nation. Broken down into five major pillars each one highlighting a different task that needs to be accomplished to reach the goal of creating a safer cyberspace. This strategy emphasizes the importance of protecting critical infrastructure as well as recognizing the importance of it. Implementing these five pillars and the strategies with each pillar should ensure that the nation's critical infrastructure is protected, and the nation's interests are being met.

References

Office of Management and Budget - The White House. (n.d.-b). https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

National Cyber Workforce and Education strategy - the white house. (n.d.-a). https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

What business needs to know about the new U.S. cybersecurity strategy. Harvard Business Review. (2023, April 14). https://hbr.org/2023/04/what-business-needs-to-know-about-the-new-u-s-cybersecurity-strategy