Justin Graham

11/05/2023

CYSE425W

Midterm Assignment

The internet is an unprecedented innovation that the world has never quite seen before in all of its history. As stated by the National Cybersecurity Strategy, “In a single generation, it has revolutionized the way we innovate, communicate, and share information on a global scale, catalyzing unprecedented advancements in human prosperity, equality, and connectivity.” (Strategy, 2023, p.1). The National Cybersecurity Strategy from 2023 highlights important concepts that have become highly relevant in today’s cyberspace. The main key concepts from this include new trends in businesses that can lead to higher risk factors, malicious actors, and the responsibility of whom to defend the Unites States cyberspace.

The first important concept it discusses is new trends used by businesses and individuals to enhance their companies utilizing the internet and cyberspace. New technologies have allowed companies to have workers work full time remotely, store all their data virtually, and add new software and systems to their companies. New technology also allows sectors to work together with others from around the world, but this comes with new cyber risks. It only takes one password being compromised, one insider threat, or one attack that can bring down a business, compromise many end users, and effect multiple nations. An example used by the strategy was “NotPetya” that originally affected “Ukraine, which then spread across Europe, Asia, and the Americas, causing billions of dollars in damage.” (Strategy, 2023, p.2).

This leads to the second key concept, malicious actors. Malicious actors are the individuals or groups that use the internet to hack others, spread false information, and steal data or money. These can be government sanctioned groups or individuals with too much free time and want to break the law. They are the biggest threat to cybersecurity in today’s age. According to the strategy, the “governments of China, Russia. Iran, North Korea, and other autocratic states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms.” (Strategy, 2023, p.3). This shows that it is not just individuals that are out to harm average internet users across the United States.

The third main concept and the main mission of the National Cybersecurity Strategy is to define and strengthen their five main pillars of cybersecurity. These include “defending critical infrastructure, disrupt and dismantle threat actors, shaper market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals.” (Strategy, 2023, p.4). These pillars are strong goals that will help align the public and private sectors of cybersecurity to help maintain a good defense around the United States and their cyberspace. They ask that the best specialists in cybersecurity step up to head the sectors and protect this country’s assets and the people within it. Only together with the government and private sector working together can this be achieved. They want to build a future where cyberspace is more protected and build upon their current policies to make this happen. They said, “This strategy’s goals for securing Federal systems and collaborating with the private sector build on EO 13800, Strengthening the Cybersecurity of the Federal Networks and Critical Infrastructure, EO 13691, Promoting Private Sector Cybersecurity Information Sharing, and EO 13636, Improving Critical Infrastructure Cybersecurity.” (Strategy, 2023, p.6).

For the next section of this paper, I will focus on Pillar One – Defending Critical Infrastructure because I believe this is one of the most important parts of the strategy as every person in the United States relies on critical infrastructure (CI) in their daily lives. One of the reasons CI is highly prioritized by both national security and malicious actors is that CI affects people every day. If some of these systems were taken down, society itself could come to a halt. Imagine if the energy grid was taken out for a few days, it would spell disaster and chaos for the surrounding areas. This pillar focuses on the collaboration of private sectors who owns critical infrastructure working together with federal agencies to ensure better cybersecurity practices are in place as well as making sure critical infrastructure systems are more “defensible and resilient”. (Strategy, 2023, p. 7).

One of the major concerns surrounding critical infrastructure is the lack of mandatory regulations required by CI companies. The strategy emphasized that the lack of regulations has led to “inadequate and inconsistent outcomes” (Strategy, 2023, p.8) regarding cybersecurity. With a new focus on this pillar, new cybersecurity requirements that can unify the security measures in our CI would lead to better regulation and a stronger cybersecurity defense. It stated, “The administration has made progress in this area, establishing cybersecurity requirements in key sectors such as oil and natural gas pipelines, aviation, and rail, led by the Transportation Security Administration and water systems, led by the Environmental Protection Agency.” (Strategy, 2023, p.8). This is a good start for establishing a baseline of policies for cybersecurity practices throughout much of the United States CI systems.

Another main objective of the Defending Critical Infrastructure Pillar is to scale the public and private sector collaboration. Sometimes, private sectors can develop better security measures because they have more funding or employees that can help develop new policies and software. This is promoted through healthy competition of businesses and higher pay can entice the experts in the field to work for these companies. However, each company wants to stay ahead of their competition and will not share their secrets with others. This is where the pillar is looking to have those experts help the public/federal sector by sharing information to make a coordinated effort to help protect critical infrastructure security. The strategy hopes to have “the Federal Government deepen operational and strategic collaboration with software, hardware, and managed service providers with the capability to reshape the cyber landscape in favor of greater security and resilience.” (Strategy, 2023, p. 10). This will hopefully lead to real time data sharing and threat response that will strengthen the cyberspace surrounding the United States CI systems.

Although many of the CI companies can “mitigate most of the cyber incidents without help from the federal government, the Federal government must present a unified, coordinated, whole of government response.” (Strategy, 2023, p.11). This sums up most of what this pillar wants. The government wants to be able to help unify the critical infrastructure systems with coordinated efforts between the private and government sector to ensure the best cybersecurity defense is possible. They hope to establish new and revised regulations that will result in the most resilient defense possible and allow the United States critical infrastructure system to continue operating as safely and efficiently as possible.

References:

National Cybersecurity Strategy, March 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>