An Overview of the National Cybersecurity Strategy and the Pillar of Critical Infrastructure

The National Cybersecurity Strategy

The 2023 National Cybersecurity Strategy published by the White House seeks to go over the five pillars of building a digital ecosystem together through collaboration with other countries, and making national cybersecurity more easily and inherently defensible, resilient, and aligned with our values. The strategy also goes over the ever deepening digital dependence of the modern world, which I wholeheartedly agree with. The age of the internet of things and rapid expansion in improvements in internet, cyber operations, and day to day operations regards it as a matter of extreme importance. As we enter further into the age of IoT, it is apparent not only our current systems must be upgraded to better fit and protect, but our older systems as well, which the strategy goes over. As potential malicious acts can come from all forms and places, it is very much required that end users may not be extreme factors to breaches of national security, and instead a rebalancing towards more secure sectors is far needed.

The Five Pillars

The five core pillars of our national cybersecurity strategy are as follows; defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals. The first pillar, defending critical infrastructure, is one I believe to be of the most importance towards our core national cybersecurity strategy. Government collaboration with private sectors on security practices is one of the strongest ways to further build security across the nation's most common sectors at the fastest pace. Think of it as scientists working together to create a

cure for a disease, the more collaborators, the quicker the entire process goes. Pillar two, disrupt and dismantle threat actors, is also of great importance. The United States in the past has collaborated with other foreign nations to disrupt potential threats, such is the case with StuxNet, where the U.S. and Israel collaborated to make a worm virus which dismantled and destroyed key Iranian nuclear infrastructure (Fruhlinger, 2022). This pillar also seeks for collaboration between public and private sectors for faster incident response and victim notification. A main thing of note is how this sector seeks to mainly counter cybercrimes, and most notably defeat ransomware, even creating the Counter-Ransomware Initiative (CRI) to help with this task. I believe ransomware is one of the most damaging types of cyber attacks that can occur, so I am extremely happy with the U.S.'s clear focus on countering it. Pillar three, shape market forces to drive security and resilience, seeks to reduce the risk of potential attacks of cyber markets through accountability. One of the main focuses of this pillar is the greater security of IoT devices, through potential federal grants and other avenues of security enhancement. IoT is one of the strongest security weaknesses currently across the board due to the extreme lack of security on most of them. I believe this pillar is the most suited to protecting the public from cybercrime and breaches. Pillar four, investing in a resilient future, seeks to create investments now which will greatly benefit us in the future. This pillar I believe is one of the weaker ones, as most of what is gone over is done on all other pillars, as it seeks to reinvent policies and further develop potential avenues towards our future, leading to most of it being guesswork. Pillar five, forge international partnerships to pursue shared goals, as it suggests, seeks to form foreign partnerships to pursue related cybersecurity goals. This pillar seeks to help through collaborative threat protection groups, and the securing of global supply chains. I believe this pillar is another

one which seeks to further build security through the resources of many partners, all for furthering the nation's defense.

Implementation

The U.S. seeks to implement this strategy through a data-driven approach, with a key monitoring of potential threats and resources. This strategy also seeks to learn from the past cybersecurity mistakes of our country and use them as a stepping stone to further move to a stronger tomorrow. I believe a data-driven approach towards this strategy will work however, some pillars of the strategy may take a lot longer than others to see agreeable results. It must also be considered about outside factors which may make it harder for some strategy parts to be implemented.

A Further Dive into Pillar One

Pillar one, defending critical infrastructure, requires a keen collaboration between federal, private and public sectors to be as secure as possible. While this does not mean I believe corporations should know the way we protect our water or power plants, I believe stronger protections against normal cyber attacks or breaches would be of a much greater importance. Further collaborations between public and private sectors would greatly help improve citizen confidence and deepen security. The implementation, moderation, and regulation of federal cybersecurity centers across the country would also greatly help deepen national security.

The Importance of Defending Critical Infrastructure

I believe defending critical infrastructure is by far the most important pillar of the entire strategy. It can be argued all of the pillars, bar potentially pillar five, all require pillar one to be at an expected point before they can be properly implemented. Critical infrastructure, the operations that protect our daily way of life, that if taken away would immediately be noticed are

of the most importance. One of the glossed over aspects in our public is the re-strengthening of our past systems and infrastructure to a modern level. Our critical infrastructure, like power or water plants running on old tech from around 20 years ago is not acceptable, and must quickly be updated to better fit our modern times. As critical infrastructure being attacked and either destroyed or shut down by foreign attacks would be the most damaging towards citizens and our country, having the strongest defenses placed onto them would maintain citizen morale and allow for greater responses. These places of critical infrastructure, which I would argue now include places of internet or high level databases, must properly be maintained and secured through any possible passage. Take for example the recent Shanghai database breach. This breach, potentially one of the largest in history, which held over 24 terabytes of chinese citizen's personal information, was all caused due to a high ranking official leaving his password on a data blog. The attackers upon using this password found out the database itself had no proper protections like a password or any data transfer monitoring (CSM, 2022). This leak of information could damage the lives of millions of Chinese citizens, who must use their own social credit score to even live their daily lives, through identity theft and other means of cybercrimes. This is why I believe it is of the utmost importance that critical infrastructure like water, electricity, internet, and private information must be secured. As leaks or shutdowns of any of these can result in huge civilian unrest or backlash, and can extremely damage the way of lives of American citizens.

References

Fruhlinger, J. (2022, August 31). *Stuxnet explained: The first known cyberweapon*. CSO Online. Retrieved March 19, 2023, from https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html#:~:text=What%20is%20Stuxnet%3F,about%20its%20design%20and%20purpose.

The Christian Science Monitor. (2022, July 6). *Shanghai Data Leak: China tested by possible largest hack in history*. The Christian Science Monitor. Retrieved March 19, 2023, from https://www.csmonitor.com/World/Asia-Pacific/2022/0706/Shanghai-data-leak-China-tested-by-possible-largest-hack-in-history