The U.S Government's Strategic Plan for Creating a National Cyber Security and Communications Center

Introduction

The security of assets and data for organizations is of the utmost importance in today's world. Security breaches can cause the loss of data and can cause devastating losses in operations and finances, which can then decrease their market value and tarnish their reputations. Since this has become more and more apparent, organizations and companies are compelled to invest in or seek out services in cybersecurity to better protect their physical and digital assets from being destroyed or stolen. In recent years, the frequency of cybersecurity incidents has only increased and shows no signs of going down, which calls for the development of new security policies and the refining of old policies that are still in place.

Overview

Back in 2014, the U.S Government refined the Homeland Security Act of 2002 and created a new document entitled the National Cybersecurity Protection Act of 2014. This act allowed the Department of Homeland Security to create a National Cybersecurity and Communications Integration Center in order to carry out the duties and responsibilities of the DHS in regard to infrastructure protection, cybersecurity, and other DHS related programs. The act states that the center was to become a "federal civilian interface" (Hunton and Williams, 2014) and aid federal and non-federal organizations with normal cybersecurity tasks and other technical assistance. This made the DHS's NCCIC the federal government's central hub for public-private cybersecurity information sharing. Some of the highlights of the bill are as follows (Hunton and Williams):

1) "Codifies DHS's National Cybersecurity and Communications Integration Center ("NCCIC") as a federal civilian interface" to provide federal and non-federal entities "shared situational awareness" to address cybersecurity risks, coordinate the sharing of cybersecurity information, conduct and share analysis, and provide technical assistance and recommendations on network security.
2) Directs that NCCIC should include members of sector-specific agencies, law enforcement, the intelligence community, state and local governments, information sharing and analysis organizations, and owners and operators of critical information systems.
3) Directs DHS to make available the process to apply for security clearances to those involved in public-private information sharing.
4) Makes clear that nothing in the Act shall be construed as providing new regulatory authority."

As of right now, the implementation of the NCCIC has proven to be one of our greatest assets in the field of cybersecurity and communications. There are several benefits to having this sort of system in place. The NCCIC has an on-hand incident response team that aids the federal and non-federal entities when there is a breach or any other crises.

Reason for Development

In recent years, the sheer number of cyber related attacks and breaches has only increased, causing uncertainty with the protection of data and other sensitive information. Something that has been developed for this very reason was the basis of this act, the National Cybersecurity Protection System. This system relies on the tight collaboration and integration with stakeholders in order to support the defense of their underlying networks. There are four

broad technology areas in which the NCPS has capabilities: intrusion detection, analytics, information sharing, and intrusion prevention. The intrusion detection systems are relatively simple to understand. It is “a passive, signature-based sensor grid that monitors network traffic for malicious activity to and from participating departments and agencies” (CISA 2021). To go along with intrusion detection, the NCPS also has capabilities for intrusion prevention. This allows the NCPS to easily identify and categorize any malicious network traffic that comes through as a way to strengthen cybersecurity analysis and security response. However, this still remains as a problem today. With more advanced hackers and malware, more sound cybersecurity systems are needed. Unfortunately, even with those advanced systems, nothing can be 100% secure and protected, so there is still risk involved when it comes to securing data and information.

How this Strategy Fits Within a National Cybersecurity Policy

In 2014, this act was the start of a centralized hub for cybersecurity within the private and public sectors. Collaboration between federal and non-federal entities was occurring without any problems and they were working towards a more secure infrastructure. Today, this act is still relevant, and it continues to be amended to fit the needs of today’s world of technology.

"Congress Passes Four Cybersecurity Bills - Hunton Andrews Kurth." *Hunton and Williams*, 2014, https://www.huntonak.com/images/content/2/4/v3/2499/congress-passes-four-cybersecurity-bills.pdf.

"National Cybersecurity Protection System." *Cybersecurity and Infrastructure Security Agency CISA*, 2021, https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

"Text - S.2519 - 113th Congress (2013-2014): National Cybersecurity ..." *Www.congress.gov*, 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2519/text.