Political Implications of The Cybersecurity Enhancement Acts

Introduction

With the ever-evolving nature of cyberspace and other related environments, governments, private sector and associated organizations, and users all over the world may face more and more frequent cyber-attacks. While there has been protections and other safeguards that have been established, no computer or device is perfectly safe and secure. The government policies and procedures only protect users for so long. The cybersecurity enhancement acts that have been revised and introduced have done so much for the field and what protections the government, organizations, and users/families have over their information and devices. This paper will delve into the finer details of what the political implications and ideas were behind some of the revisions of this act.

Who is in Charge of the Legislation and Law Revising?

The act was created for the collaboration between the public and private sectors since there was a sizable gap between the two before regarding cybersecurity. The reins were given to the Director of NIST (National Institute of Standards and Technology) as well as the Secretary who acts through the director. In the earlier revisions of the act, the Department of Homeland Security (DHS) was chosen to become the national hub for cybersecurity and communications. Entities that are in charge are also heavily based on which political parties are in charge of the House and the Senate. Both groups seem to agree that cybersecurity should be shored up more and more each year as we experience more complex cyber-attacks throughout the year. To put the situation regarding the politics and control of cybersecurity into perspective, “There is a “turf war” in the cyber security field between the Department of Homeland Security, the National

Security Administration, and the Pentagon" (Stone, 2). This really shows how even back in 2009, there were several disputes between government agencies about the sole control of cybersecurity and how those organizations sought to run things.

Strategies and Concerns

In the 21st century, there have been so many strategies and other acts that have been developed in hopes to shore up cyber security. One of those acts was the Cyber Security Act of 2012 and it was designed to create and establish communications between the government and companies in the event of a cyber-attack. This act also designated DHS as a regulating force and authority for cyber security along with several other federal agencies. With the assistance of NIST, DHS and the other federal agencies would conduct several tests of the cyber networks to assess and determine what the biggest risks in America's cyber security (Stone, 3)

Because of the involvement of all of these agencies and departments of the government, a bit of resistance was met with some of the suggestions that these groups came up with, as one would expect. Power struggles and relationships were tested when it came to coming up with and writing these cyber security policies. "Turf wars, executive orders, legislative procedures, patriotic culture, public backlash, and a major realignment of power within the federal government have all significantly affected cyber security policy" (Lapke & Subramanian). This just goes to show you that a lot goes into creating cohesive policies and procedures, especially with something as sensitive and complex as cyber security.

Another way of shoring up cybersecurity policies could be in the form of a sort of R&D strategy. This one is a bit experimental seeing how these policies can range from simple to very complex in a matter of seconds. "Neither the commercial marketplace nor government programs

have been successful in providing ways to protect computer systems. Transforming the cyber landscape calls for a coordinated R&D strategy that provides a basis for steering security R&D toward global strategic goals" (Benzel) This idea expresses that these policies should go through an extensive trial of research before being implemented as laws or legislations. The problem that can be seen with this strategy is the timeframe in which the testing and changing the policies could take. Each and every day the U.S. is subject to some sort of cyber-attack or data breach. A lengthy process for testing the waters with cyber policies could be spent better by creating or thinking of ways to secure information and other knowledge from possible threat.

Consequences

While the relationships between the different agencies have improved, it still remains difficult to create sound policies for cyber security. Each individual party has their own way of coming up with ideas for policies and procedures to ensure safety and security for all networks and other aspects of cyberspace. When there is any form of turmoil or animosity when developing these policies, they may not even end up being completed and might get sent unfinished, creating more work for whoever examines the policy before it is sent off to someone of higher authority.

Works Cited

Benzel, T. (2015). *A strategic plan for cybersecurity research and development*. IEEE Xplore. Retrieved October 2, 2022, from https://ieeexplore.ieee.org/abstract/document/7180232

Lapke, M., & Subramanian, R. (2014). *Power relationships in the United States federal government and its ...* researchgate.net. Retrieved October 3, 2022, from https://www.researchgate.net/profile/Michael-Lapke/publication/275271473_Power_Relationships_in_The_United_States_Federal_Government_and_Its_Effect_on_Cybersecurity_Policy/links/553fb23e0cf2320416ebc102/Power-Relationships-in-The-United-States-Federal-Government-and-Its-Effect-on-Cybersecurity-Policy.pdf

S.1353 - Cybersecurity Enhancement Act of 2014 113th ... - congress. (n.d.). Retrieved October 3, 2022, from https://www.congress.gov/bill/113th-congress/senate-bill/1353

Stone, H. (2012). Political Strategy for Cyber Security. *Intersect*, *5*(1).