Overall Effectiveness of Cybersecurity Enhancement Acts

Introduction

With cybersecurity becoming one of the most important topics and strategy items for all countries on the planet, each law that has been created has the chance of being criticized and talked about both positively and negatively depending on what was outlined in the act. Each act that has been sworn into law or practice has been judged and remedied to meet the expectations of all those who abide by it and employ it in their workplace or society. Sometimes these acts are met with resistance because of certain aspects that have been mentioned in the act itself but most of the time, they are usually well received and followed by the vast majority of those who it involves.

Overall Effectiveness of the Cybersecurity Enhancement Act of 2014

Many groups across the United States agreed that this act was beneficial for the most part. Industry-led cyber standards were becoming more popular and had the backing of the government and many other groups across the world, like NIST and DHS (Hunton). One of the benefactors of this act was the Automation Foundation. Their chair for government relations, Steve Huffman, stated that, “by raising its importance among lawmakers, industrial cybersecurity became a more vital part of the legislation passed by Congress” (Patel). This was a sign of good news to come from this act and those that came after it. Legislation took cybersecurity more seriously when drafting later acts and documents for information security and other means of securing data. On the other hand, a law firm Hunton and Williams LLP, explained that the unexpected flurry of laws that were passed in 2014 were “limited in scope than measures sought by the private sector.” (Patel) This firm was concerned that the acts would impose and make past

and pre-existing actions official since they hadn't been at the time. Back in 2014, a report was generated for a lot of prior legislations that groups thought could be updated and revised to better prepare for cybersecurity in the modern world.

Notable Issues with Early Cybersecurity Acts

A notable problem outlined by the report was "Cybersecurity Workforce," which entails the workforce that existed ten years ago and the future generations of cybersecurity professionals (CRS Report). Proposals were made to attempt to fix these problems. An interesting proposal came through that outlined the need for addressing educational needs for the development of next-generation cybersecurity professionals. This is where the idea for the NSF/DHS Scholarship-for-service program came from and the introduction of cyber competitions to test the skills of cyber students. Some even came from the white house such as the use of public/private sector personnel exchanges, which allows for the cooperation of both private and public workforce members in order to get things done in an efficient way, and the proposal to provide additional federal hiring and compensation authorities as a way of kind of "perfecting" the hiring process of cybersecurity professionals. Another recommendation that was made for future legislations had to deal with the establishment of federal occupational categories for cybersecurity workers. This is understandable in some regards, as it can be hard to determine what part of the workforce you are a part of. You could be Information Technology, Information Security, Database Management; just to name a few, and countless others. This was a way to keep track of employees with projects and other tasks that had been assigned to them.

Overall Thoughts

Thinking that this act was one of the many passed back in 2014 that laid the groundwork for new age cybersecurity laws and acts today, this was very effective when you think about it. It may not have been effective when it was first introduced but it was refined and used later for the laws and legislations that are in place today. These acts have allowed us to make cybersecurity one of the most important areas for legislation ever. It won't be going away anytime soon either. As long as we have computers and other devices to keep secure, cybersecurity will never go extinct. We will always need some sort of backing and ways to keep breaches and information leaks from happening.

Works Cited

"Congressional Passage of Cybersecurity Bill Is a Triumph for Automation, Groups Say." POWER Magazine, 18 Dec. 2014, https://www.powermag.com/congressional-passage-of-cybersecurity-bill-is-a-triumph-for-automation-groups-say/.

"Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation." EveryCRSReport.com, Congressional Research Service, 12 Dec. 2014, https://www.everycrsreport.com/reports/R42114.html.

LLP, Hunton Andrews Kurth. "In a Surprising Move, Congress Passes Four Cybersecurity Bills." Privacy & Information Security Law Blog, 27 May 2020, https://www.huntonprivacyblog.com/2014/12/12/surprising-move-congress-passes-four-cybersecurity-bills/.

S.1353 - Cybersecurity Enhancement Act of 2014 - Congress. https://www.congress.gov/bill/113th-congress/senate-bill/1353.