Ethical Implications of the Cybersecurity Enhancement Acts

Introduction

Every policy and law that get introduced to both houses of Congress or even signed into law by Congress are usually met with some sort of ethical spiel about the problems that may arise from the passing and implementation of said law or policy. Many of the comments that are made about policies and laws are that they need to be revise in order to include all parties that may be involved in the ramifications of the law or policy rather than leaving them out. Ethics and morality are almost always considered when drafting laws and policies regardless of what the topic of them may be. However, there is always the risk that something may be overlooked or left out of the law or policy. With that said, the Cybersecurity Enhancement Act of 2014 was not met with a lot of ethical or moral backlash, but some could argue that it does in some areas.

Ethical Implications of the Cybersecurity Enhancement Act of 2014

As mentioned before, this act was not met with a lot of ethical or moral backlash, but some can argue that it does. Something that can be considered an ethical implication from this act was the mention that everyone, not just the government sector, was to report all possible instances of cyber threats to the DHS as it became the national hub for all cybersecurity related things and communications. This can be seen by some as an invasion of privacy or even a violation of the company's information confidentiality agreement.

Costs and Benefits of the Cybersecurity Enhancement Act of 2014

There are many benefits that accompany this cyber policy in addition to a national hub being created for the reporting of potential breaches or similar incidents and a way of communicating through a known entity such as the DHS. One of the biggest benefits/outcomes

of this cyber policy was the promise of “increasing public awareness of cybersecurity, cyber safety, and cyber ethics with the help of the creation and implementation of a national cybersecurity awareness and education program” (Cybersecurity Enhancement Act of 2014). This would be very useful to those who are either just entering the field of cybersecurity or those who want to continue to learn about the major changes that occur in the field every year.

Types of Rights that are Protected and Limited by this Policy and Individual Rights

According to an article published by Congress, describing what this act is, states that the act will work towards mitigating the impacts on business confidentiality and protect individual privacy and civil liberties, among other things (Rockefeller, J). This means that individual privacy rights will be protected along with the confidentiality rights that belong to businesses and companies. This will also protect to some extent the information security rights held by individuals and businesses alike.

Works Cited

A, N. “Cybersecurity Enhancement Act of 2014.” *Www.govinfo.gov*, Aug. 2022, https://www.govinfo.gov/content/pkg/COMPS-12455/pdf/COMPS-12455.pdf.

Radziwill, Nicole M., and Morgan C. Benton. “Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management.” *ArXiv.org*, 9 July 2017, https://arxiv.org/abs/1707.02653.

Radziwill, Nicole M., and Morgan C. Benton. “Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management.” *ArXiv.org*, 9 July 2017, https://arxiv.org/abs/1707.02653.

Rockefeller, John. “S.1353 - Cybersecurity Enhancement Act of 2014 113th ... - Congress.” *Www.congress.gov*, July 2013, https://www.congress.gov/bill/113th-congress/senate-bill/1353.