CYSE 495 Week 3 Assignment

Alexander Gardner

Old Dominion University

Understanding and Maintaining Compliance

From my own personal understanding, compliance is a major part of many cybersecurity strategy. It can be seen in industries like banking, the medical field, and more. One compliance law that sticks out to me the most is HIPAA because I have family that work in the medical field, and they keep me updated whenever they see or hear cybersecurity at work. Another compliance law that sticks out to me is the new Cyber Resilience Act in the EU. This act brings a complete overhaul of the compliance standards for all IoT devices in the EU. In this chapter, I learned more about compliance laws like Federal Information Security Modernization Act, Health Insurance Portability and Accountability Act, Gramm-Leach-Billey Act, Sarbanes-Oxley Act, Family Educational Rights and Privacy Act, and the Children's Internet Protection Act.

The Federal Information Security Modernization Act passed in 2002 enables federal agencies to protect their data and privacy. It creates a powerful team of the Department of Homeland Security and the Office of Management and Budget with a common goal of implementing information and security standards for all the federal information systems. This act also makes agencies responsible for protecting their systems and information, complying with the act, and putting the security measures into place. This act also puts into effect an annual inhouse inspection of their effectiveness and to put out a report on their compliance.

The Health Insurance Portability and Accountability Act or HIPAA is one that sticks out to me due to the family connection. HIPAA, which was enacted in 1966, ensures the protection of health information and enhancing the security measures in place. In this act there are three categories administrative, physical, and technical. The administrative category sets the standard that only people who need to access the data can access the data. The physical category sets the physical standards for the data so nobody can walk in or break into the systems holding the data.

The technical category sets the technology standards for protecting the systems. The act also sets into place a compliance plan which begins with an assessment on if the organization is covered under HIPAA. Following this a risk analysis is performed on the organization which leads to the plan's creation and implementation. Once this is done the systems are continuously monitored for changes or new threats and another assessment is done to see if their new plan is effective.

The Gramm-Leach-Billey Act may sound like a cool new folk band, but it aims to set the standards for banking and insurance organizations. This act puts into place two big rules: Financial Privacy rule and the Safeguards rules. The financial privacy rule puts the responsibility of educating the consumer of their practices of data collection and sharing on the organization. The safeguards rule enforces the organization to create a security plan to protect their information, maintain the integrity of that data, and prevent events like data breaches.

The Sarbanes-Oxley Act or SOX was enacted in 2002 applies to publicly traded companies and more particularly the board members and organization's executives. The main goal of this act is to prevent fraud. To do this SOX requires CEOs and CFOs to verify and validate the accuracy of financial statements.

Family Educational Rights and Privacy Act of 1974 protects the student's data. This act only applies to educational organizations that receive funding from the U.S. Department of Education. This act gives parents or adult students the right to inspect records and even request a correction. This act also safeguards the student's personal identifiable information by requiring parental or a students consent to release it.

The Children's Internet Protection Act of 2000 aims to restrict the access of obscene pictures or child pornography, monitor the activity of minors online, and to implement an online

safety policy for these minors. This act also only applies to schools and libraries that are funded by the E-Rate program.

The Children's Online Privacy Protection Act of 1998 protects the privacy of children who are under the age of 13. With this act, websites are required to obtain parental consent to collect or use the information of children, put into place a privacy policy, and comply with the security standards for children's online privacy and safety.