THE LAWS OF CYBERSECURITY

Protecting the 'net

Cybersecurity is a vast field that affects me, you, and everyone else. As a result of its wide-spread influences, several laws have been enacted that specifically target the cybersecurity industry. This handout will give a brief overview of pertinent laws.

SOX

Known as the Sarbanes-Oxley Act, the act intends to protect investors from fraudulent financial reporting by corporations. It holds the accountants in charge of your money, well, more accountable!

GLBA

The Gramm-Leach-Bliley Act of 1999 ensures that financial institutions communicate with customers on how their private data is protected and used. You want to make sure the place keeping your money safe also keeps you safe!

HIPAA

The Health Insurance Portability and Accountability Act enforces strict stipulations on how personal data is used by healthcare industries. You trust a hospital to take care of you, so you also need to be able to trust them with your data!

ECPA

The Electronic Communications Privacy Act protects information while it is stored or is in transit. Essentially, it prevents illegally obtained communication logs/transcripts being presented as evidence, and stops the collection of it in general.

CFAA

The Computer Fraud and Abuse Act is the primary law to think about when it comes to crimes involving technology. It is essentially the grandfather of most technology laws.

US PATRIOT

The United States Patriot Act was enforced after the September 11, 2001 terrorist attacks on the World Trade Center. It gives the government more power over data collection and usage.

NERC CIP

Rather than focusing on data itself, the NERC CIP standards focus on the electrical grid, and the means with which a company should secure it. A firewall isn't really helpful if you can't power it!

PCI DSS

The PCI DSS standard is a guideline for security concerning credit cards, including cardholder data, network and system security, and general auditing standards. This standard is used widely across all fields, due to how important the use of credit cards are.

The NIST Standard

The NIST organization assembled the Cybersecurity framework, consisting of five key functions detailed below. They represent the five primary pillars for a successful and holistic cybersecurity program.

Identify

- Establish an Asset Management program
- Identify the cybersecurity capabilities of the organization
- Identify asset vulnerabilities

Protect

- Protections for Identity Management and Access Control
- Establish Data Security protection consistent with the org's risk strategy
- Manage Protective Technology

Detect

- Ensuring Anomalies and Events are detected
- Implementing Continuous Monitoring capabilities to monitor for events
- Maintaining Detection Processes to provide awareness of events

Respond

- Ensuring Response Planning processes are executed during and after an incident
- Mitigation activities are performed to prevent expansion of an event
- Analysis is conducted to ensure effective response and support activity

Recover

- Ensuring the organization implement Recovery Planning processes and procedures
- Implementing Improvements based on lessons learned and reviews of existing strategies
- Internal and external communications are coordinated during and following a cybersecurity incident