Alexander Cannell

11/27/2016

CSIA 6000

Laws and Regulations

**Identify the Laws/Regulations that affect your current organization's operations.**

I work for Ancestry.com and here are laws I know apply to us:

* Communication Assistance for Law Enforcement Act of 1994 (CALEA)
* Controlling the Assault of Non Solicited Porngraphy and Marketing (CAN SPAM)
* Electronic Freedom of Information Act of 1996 (E FOIA)
* Electronic Communications Privacy Act of 1986 (ECPA)
* Electronic Funds Transfer Act (EFTA)
* Financial Industry Regulatory Authority (FINRA)
* Federal Information Security Management Act (FISMA)
* Federal Trade Commission Act (FTCA)
* Federal Privacy Act of 1974 (FPA)
* Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
* Health Insurance Portability Act (HIPAA)
* Health Information Technology for Economic and Clinical Health Act (HITECH)
* Office of Foreign Assets Control (OFAC)
* Payment Application Data Security Standards (PA DSS)
* Payment Card Industry Standard (PCI DSS)
* Privacy Protection Act of 1980 (PAA)
* Right to Financial Privacy Act of 1978 (RFPA)
* California Senate Bill 1386
* Sarbanes-Oxley Act (SOC)
* Federal Identity Theft and Assumption Deterrence Act
* NASD Rule 3110
* Sec Rule 17a-4
* Title 21 Code of Federal Regulations Part 11

We have a lot of others for international because we are an international company. Like the EU’S Data Protection Directive (Directive 95/46/EC) I was able to talk with Ancestry’s in house Attorney told me he would send me more laws but he never got back to me on it. Sad day! I will update you when I get that information.

**Outline what your security team needs to do in order to comply with the Laws/Regulations.**

As Professor Robertson said in our class on monday meeting government law standard doesn't mean you are secure; It just means you are compliant. The book mentions the Target Breach in 2013 as an example of the consequences of what might happen if you are not compliant. I think that the Target Breach was a definable changing point in Corporation Security. Where Corporations seem to be more concerned now about security, and addressing security as a real concern. The Target Breach is kindof the poster child of what you don't want to happen, even though similar POS data breaches continue to happen. But it is pinnacle events like the Target Breach that help us move forward to an state of reasonably secure as a company. Which brings me to one thing we could do as a security team to be more Industry compliant is to be up to date on current incidents/breaches and countermeasures. It will save the company money and time in the future if we were up to date.

Compliance means conform with a law, specification, policy, or standard. The Book gives two standards of compliance first Regulatory, and Industry Compliance which are essentially the same thing. Regulatory Compliance is an adherence to “regulations” that are specific to what the company/ organization does both with employees and customers; these regulations can be laws, guidelines and specifications. For example I use to work for a hospital we had to be both HIPAA and HITECH compliant to protect patient confidentiality but those two compliances also cover employee confidentiality; I.E: Health insurance. Regulatory is typically mandated by law.

Industry Compliance encompuses regulatory compliance meeting legal guidelines but with the added security of Best practice and Industry guidelines. I.E: PCI Compliance. Industry Compliance or the best practice compliance is an industry standard typically more secure than Regulation compliance. As a security team we can make sure we understand the laws and regulations specific to our company making sure we are compliant with those laws and regulations at a industry standard. A down side to industry compliance is that industry compliance could prevent a company doing business. Inshort: compliance protects businesses from negligence.

Security and compliance are not the same thing. Proper security protects your information, but compliance is a method of demonstrating how your company's security program meets specific standards. An amazing security program should produce compliance. We as a team need to focus on being at a state of reasonably secure which in turn will yield a result in being compliant. As a security team, we can be compliant by understanding our system, understanding our vulnerabilities, taking preventative measures, understanding the compliance requirements for the organization, and understanding/performing the six primary phases in incident handling procedures.

**References:**

* Hagerman, K. (2016, February 20). Security vs. Compliance | ARMOR Resources. Retrieved October 30, 2016, from https://www.armor.com/resources/security-vs-compliance/
* Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (2nd ed.). Syngress.