Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

Laws and Regulations

- Speaking specifically in the context of information security the body of applicable laws and regulations with which we, as information security professionals, might potentially need to concern ourselves with is massive. In the world of physical incidents, such issues, although still potentially complex, are much more straightforward and more easily enforceable.
- The laws are always playing catchup to the reaility of the digital cyberscape.

Laws and Regulations

- FISMA: The Federal Information Security Modernization Act (FISMA) provides a framework for ensuring the effectiveness of information security controls in government. This legislation is intended to protect government information, operations, and assets from any natural or manmade threat. FISMA requires each federal agency to develop, document, and implement an information security program to protect its information and information systems. Annual reviews of these programs are required to maintain compliance and keep security risks to an acceptable level.
- FERPA: The Family Educational Rights and Privacy Act (FERPA) protects the privacy of students and their parents. FERPA requires all schools that receive funds from programs administered by the U.S. Department of Education to comply with standards regarding the disclosure and maintenance of educational records, including educational information, personally identifiable information, and directory information. FERPA also grants certain rights to students and parents regarding the student's own records.

Laws and Regulations

- SOX: The Sarbanes-Oxley Act (SOX) regulates the financial practice and governance of corporations. SOX is designed to protect investors and the general public by establishing requirements regarding reporting and disclosure practices. The act mandates standards in regard to areas such as corporate board responsibility, auditor independence, fraud accountability, internal controls assessment, and enhanced financial disclosures. SOX also established the Public Company Accounting Oversight Board (PCAOB), which oversees public accounting firms and independently ensures compliance with SOX for auditing practices.
- GLBA: The Gramm-Leach-Bliley Act (GLBA) protects the customers of financial institutions, essentially any company offering financial products or services, financial or investment advice, or insurance. The GLBA Privacy Rule requires financial institutions to safeguard a consumer's "nonpublic personal information," or NPI. GLBA also mandates the disclosure of an institution's information collection and information sharing practices, and establishes requirements for providing privacy notices and opt-outs to consumers.

Laws and Regulations

- HIPAA: The purpose of the Health Insurance Portability and Accountability Act (HIPAA) is to improve the efficiency and effectiveness of the health care system. Certain provisions within HIPAA require privacy protections for individually identifiable health information, also known as protected health information, or PHI. These provisions, collectively known as the HIPAA Privacy Rule, mandate safeguards to protect patient privacy. The HIPAA Privacy Rule sets limits on the use and disclosure of patient information without authorization, and grants individuals rights over their own health records.
- Health Information Technology for Economic and Clinical Health Act (HITECH): Act was created to promote and expand the adoption of health information technology, specifically, the use of electronic health records (EHRs) by healthcare providers.

Laws and Regulations

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT): The purpose of the USA Patriot Act is to deter and punish terrorist acts in the United States and around the world.
- Electronic Freedom of Information Act of 1996 (E FOIA): require agencies to provide the public with electronic access to any of their "Reading Room" records that have been created by them since November 1, 1996.
- Computer Fraud and Abuse Act of 1986 (CFAA): is a law that was passed by U.S. Congress in 1986 to reduce the hacking and cracking of government or other sensitive institutional computer systems. The act states that anyone who engages in the following will be subject ranging from fines to imprisonment.

Laws and Regulations

- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM): Act, a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations. Despite its name, the CAN-SPAM Act doesn't apply just to bulk email.
- Children's Online Privacy Protection Act of 1998 (COPPA): imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

Laws and Regulations

- Payment Card Industry Standard (PCI-DSS): is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.
- PCI-DSS is not a law! It is industy regulating industry without government involvement.

Compliance

- Compliance means conforming to a rule, such as a specification, policy, standard or law.
- Regulatory compliance is a matter that is very specific to the industry in which a given company or organization is operating and how it is structured, although it is often more far-reaching than we might imagine. Regulatory compliance ***is mandated by law.***
- Industry Compliance In some small number of cases, we will face compliance with regulations which are ***not mandated by law***, but which can nonetheless have severe impacts upon our ability to conduct business. The primary example of this which is in common use is compliance with the PCI DSS, often simply referred to as PCI compliance.

Privacy

- Privacy is "The state or condition of being free from being observed or disturbed by other people."
- Privacy Rights: The concept of an individual's right to privacy is something that has been discussed for many years and, like any other privacy topic, is a bit of a gray area. In some countries, such as Spain, the Czech Republic, Iceland, Norway, and Slovenia, issues of privacy are considerably cleaner and clearly defined by law. On the other end of the scale, we see countries such as Bahrain, Iran, Nigeria, Syria, and Malaysia
- In the United States, one of the major privacy laws which appeared on the list earlier in this lesson is the Federal Privacy Act of 1974. This act "safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called 'fair information practices,' when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it lets individuals sue the government for violating its provisions"

Privacy and Business

- Privacy can be a very touchy concept when conducting a business, particularly regarding the handling of sensitive data.
- Personally Identifiable information (PII): PII is information that can be used to identify an individual in any search. Some examples are your name, address, social security number, payment card data, date of birth, e-mail address, phone numbers, IP addresses, MAC addresses, operating system and application information, mobile device information, biometric data, and numerous other items.
- Organizations must find was to protect the data that is collected for their data subjects. If not, the organization could face fines and damage to the public trust.