# Transcript: IT Podcast - Ep 109 - C836 Lesson 6 - with Arthur Moore and Jessica Galterio

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker # 1: Arthur Moore

WGU's IT audio series, flexible, portable, profound.

Hey, this is Arthur with WGU, I'm one of the course instructors for C836, Fundamentals of Information Security. This is Chapter 6. Let's jump into it. Just as a reminder, this series is meant to supplement the reading material, not to replace the reading material. Laws and regulations. In this particular lesson, we're going to go over the laws, and regulations that could impact us as information security professionals.

We do not need to know the laws in and out, back and forth, that's what we have legal departments for but it is noted that information security professionals need to be aware of the laws, and regulations for the industries that they are operating in. The laws will always be playing catch up to the reality of the digital cyber scape.

FISMA, the Federal Information Security and Modernization Act provides a framework for ensuring the effectiveness of information security controls in the government. This legislation is intended to protect government information, operations, and assets from any nature 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 risk to an acceptable level. FERPA, the Family Educational Rights and Privacy Act protects the privacy of students, and their parents. FERPA requires that all schools that receive funds from programs that are administrated by the US Department of Education to comply with standards regarding the disclosure, and maintenance of educational records, including education information, personally identifiable information, directory information. FERPA also grant certain rights to students, and parents regarding the student's own records. SOX is designed to protect investors, and the general public by establishing requirements regarding reporting and disclosure in practices. The act mandates standards in regards to areas such as corporate board responsibility on our independence, for odd accountability, internal controls, assessments, and enhance financial disclosures. SOX also establishes the Public Company Accounting Oversight Board. That's [inaudible 00:03:05] which oversees public accounting firms and independently ensures compliance with SOX for auditing practices. Now, for those of you that don't know, SOX comes from the Enron scandal with Arthur Johnson auditing company.

Whereas basically Enron's Governing Board played ignorance, whereas their auditor was also hired as a consultant for them. That's why Arthur Johnson is no longer around. After this particular law was brought into existence, the company ended up going bankrupt, and was disbanded along with the Enron scandal.

This is where this particular Sarbanes-Oxley Act comes from. The Gramm-Leach-Bliley Act 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 information API similar to that PII, GLBA also mandates the disclosure of an institution's information collection, and information sharing practices privacy, and establishes requirements for providing privacy notices, and opt-outs for consumers. HIPAA. One of the ones that I've worked with personally in my career is the purpose of the Health Insurance Portability and Accountability Act is to improve the efficiency, and effectiveness of healthcare systems.

Certain provisions within HIPAA require privacy protections for individuals. Individually identifiable information, also known as Protected Health Information or PHI, different from PII, this is dealing with health information. These provisions, collectively known as HIPAA privacy rule mandates the safeguards to protect patient privacy. The HIPAA privacy rule sets limits on the use of disclosure of patient information without authorization, and grants individuals the right over their own health records. High-tech Health Information Technology for Economic and Clinical Health Act. Hitech Act also created to promote the expansion, and the adoption of information technology specifically for the use of health records, EHRs by healthcare providers. Whereas you have HIPAA to protect PHI, Hitech is to modernize the health service industry.

Uniting in Strengthening America by providing appropriate tools required to intercept, and obstruct Terrorism Act of 2001, the US Patriot Act. The purpose of the US Patriot Act is to deter, and punish terrorist acts in the United States around the world. This all comes from the 2001 World Trade Center attack. The Patriot Act went into effect later on that year.

The Electronic Freedom of Information Act of 1996 requires agencies to provide the public with electronic access to any of their read room records that had been created by them since November 1, 1996. Basically, if a government agent collects information about you, you can request it through the Freedom of Information Act. The Computer Fraud and Abuse Act of 1986, the CFAA, is a law that was passed by US 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. The Computer Fraud and Abuse Act was the first law that actually came into effect, because a worm was released on a government network that actually caused a denial of service event.

Controlling the assault of non-solicited pornography and marketing material. CAN-SPAM act, a law that states, and sets the rules for commercial email establishes requirements for commercial messages, gives recipients the right to have you stop email, them stop emailing you, and spills out tough penalties for violators. Despite its name, the CAN-SPAM Act doesn't apply to bulk email. Basically, it's saying that commercial vendors that send you their marketing material have to have an opt-out button in your email. If you are getting those emails from a company that you signed up for, that you don't want anymore, you can always say opt out of the email. The Children's Online Privacy Protection Act of 1998, COPPA, imposes certain requirements, or operators of websites or online services directed to children under the age of 13, and on operators of other websites or online services that have actual knowledge that they are collecting PII, personal online information from a child under the age of 13.

Payment Card Industry Standard, PCIDSS, is a set of security standards designed to ensure that all companies that except process, store, or transmit credit card information, maintain a secure environment. PCIDSS is by a law, it is a regulating industry without government involvement. I really want to emphasize PCIDSS is not a law.

It is just in the industry regulating industry. Compliance. Compliance means conforming to a rule such as a specific policy, standard, or law. Regulatory compliance is a matter that is very specific to an 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. Regulatory compliance mandated by law. Industry compliance. In some small cases, we will face compliance with regulations which are not mandated by law, but which can nevertheless have severe impacts on our ability to conduct business. The primary example of this common use compliance is PCIDSS, referred to as PCI compliance. Privacy. Privacy is the state or condition of being free from being observed or disrupted by other people, specifically, dealing with our Fourth Amendment rights. Privacy rights. The concept of an individual's right to privacy is something that has been discussed over many years, long before information security.

Like any other privacy topic, it is a bit of a gray area. In such countries, such as Spain, Czech Republic, Iceland, Norway, Sylvania, issues of privacy are considerably cleaner and defined by law. These are more, I would go as far as the say, Western countries. Whereas we see, Iran, Nigeria, Syria, and Malaysia are on the other end of the spectrum and China as well, so those would be more Eastern countries when dealing with privacy rights. The western world is more allowing their citizens to have privacy. Whereas the Eastern world is more willing to dig in and look into the privacy or violate the privacy of its citizens. In the US, one of the primary privacy laws has appeared in the list earlier in the lesson was the Federal Privacy Act of 1974. This act safeguards the privacy through creating four procedural and substantive rights in the personal data information. First, it requires government agencies to show any individual any records kept from him or her. Second, it requires agencies to follow certain principles as fair information practices when gathering and handling data. Third, it requires restrictions on how agencies can share individuals information with other people. Fourthly, it lets individual sue the government for violating these provisions. This goes along with the Freedom of Information Act of 1996, where basically the government has to give you any information that they have on you or any government agency.

Privacy in business. Privacy can be a very touchy subject when it comes to conducting business in a particular manner. When we have PII, it is personally identifiable information that can be used to identify individual in any search. Some examples are your name, social security number, payment card information, address, date of birth, e-mail, phone numbers, IP address, MAC address, operating system, bio-metric info, mentioned mobile data, the list goes on and on. Organizations must find a way to protect this data collected for its subjects, if not, the organization will face fines and public trust. We see all too often in the news where we have a breach because of some issue with PII and some vulnerability that was overlooked. I want to wrap this up by saying that this is not an all inclusive list.

These were the biggest items that stuck out to me going through this particular lesson and in my career. I want to make sure to bring these to the forefront for anybody that is listening to this particular session. With that, I am going to wrap up and say, have a nice day. Again, I appreciate you stopping by and listening to this audio series on C836, fundamentals of information security. With this, I would challenge you to contact your course instructors if you're having any issues within the course, and apply these concepts to your daily lives and they will flow a lot easier. Thank you very much, and have a nice day.

Schedule time with your course instructor to explore more deeply. WGU, a new kind of you.