Introduction to the FTC

Welcome to 6355 Legal and compliance issues in security. We'll start the course off probably someplace you wouldn't expect by looking at the Federal Trade Commission Data Security.

Welcome to Week 1

In week 1 we look at foundations of the legal system that impact cyber security. The Federal Trade Commission Act might be the closest thing we have to a Federal Data Security Law. We'll also look at how the state data breach notification laws impact security operations of an enterprise. We'll also look at how the states have implemented data security laws and data disposal laws.

The United States is one of the few countries that doesn't have a federal standard on the minimum data security requirements. If you look at the EU, each member state adheres to a centralized data security standard that was established by the congress of the European Union. However, each state tends to add a few things to it that are specific to their view of how to manage data security within their countries. Specific industries in the U.S. have rules and statutes to direct their security practices. The financial industry has Gramm-Leach-Bliley and the Security Exchange Commission; the health industry has the Health Insurance Portability and Accountability Act; and the payments industry has the payment card industry data security standard. All three of these industries have a long history of establishing rules and regulations or working with rules and regulations through statutes that govern their protection of data and the reporting of problems that may occur with that data. The closest thing we have to a federal standard for security is Section 5 of the Federal Trade Commission Act (FTC).

The FTC aggressively enforces data security. We just said there is no federal data security law, so how do they do that? But it is true that they do. So, Section 5 of the Federal Trade Commission Act (by the way it is roughly a century old) provides for protection of consumers and competitors against unfair business practices. This is the primary tool that the FTC uses to bring enforcement actions against companies that don't take the necessary steps to protect sensitive data. We'll look at the impact that an enforcement action by the FTC can have on a company. And it can be rather substantial.

Section 5 declares illegal, unfair or deceptive acts or practices in or affecting commerce. Notice nowhere does the text of Section 5 mention data security. Remember, Section 5 of the FTC is roughly a century old, so neither were there any data security issues at the time nor were there any computers for that matter. However, it is under Section 5 that the FTC claims the authority to enforce data security actions. Now, we talk about something called the Cigarette Rule here. I started the lecture this week with a vintage cigarette ad. I hope you had a chance to look at that before you did the lecture. Rules like this were developed by the FTC as it was developing a strategy to regulate cigarette advertising. It was applied to a

case to determine if a practice that is neither deceptive nor a violation of antitrust laws is nonetheless unfair.

The 3 provisions of the Cigarette Rule are: 1) Whether the practice offends public policy as established by statutes, common law, or otherwise 2) Whether the practice is immoral, unethical, oppressive, or unscrupulous 3) Whether the practice causes substantial injury to consumers or other businessmen.

Well, when you think about it, which of these three rules do you think they use to consider enforcement actions against the companies that have data breaches? Well certainly, using number one, you look at whether a statute or common law already establishes a public policy. Using number two, you look at a motive in moral, unethical, or unscrupulous actions that could cause unfairness. Using number three, you look at whether the practice causes substantial injuries to consumers. certainly, the third point is where the primary focus of the FTC is when it comes to enforcing prosecution actions against companies.

There is an unfairness policy statement that was established by the FTC. First, the injury must be substantial. Second, the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces. And number three, the injury must be one which consumers could not reasonably have avoided. This Unfairness Policy Statement was added to the FTC Act as Section 5(n), and thus became part of the regulations.

So, how might this be applied to a data breach? Well, with substantial injury, the consumer must have significant loss. For instance, you could demonstrate you had identified theft or withdrawals from your bank account. It is not enough to necessarily just show that your data was part of the data that was compromised. The benefits outweigh the injuries. This is difficult for a company to prove. You must show that it would have been very difficult for the company to have prevented the breach. You can't argue that security was too expensive. It just doesn't fly. But you might argue that securing the data was impossible, somehow, or so costly to protect that it would have adversely impacted the consumers. Making those arguments are very difficult in today's world. Could the consumers have reasonably avoided the injury? Did the consumer do what they needed to do to prevent injury? i.e. Keep their operating system up to date or use anti-virus software-- the things that could have protected them from perhaps malware, or something that could have aided in the theft of their data.

In roughly 2015, the Wyndham Case presented a challenge against the authority of the FTC to conduct enforcement actions under Section 5. Remember, there is no Federal law that grants the authority to the FTC. We must look at what was at stake if for some reason this case had gone through. Here is the important thing… we talked about the impact of an enforcement action on a company. Here are the typical provisions of an enforcement action. The company must develop a comprehensive information security program. I think that actually is rather positive. If you don't have an information security program at that point in time, you really do

need one. The company must provide periodic independent assessments of the information security program. Many companies already do that by having independent auditors come in and look at their security programs. Certainly, I had experience with PCI DSS and we had auditors come in every year and look at how we matched up against the PCI DSS standards. Now, keep in mind, compliance to PCI DSS does not equal security. But it was a great start to ensure you had the best practices in place related to that particular standard, and you could build from there. The company must provide the FTC with access to the company's information security programs for up to 20 years. That means you are under the microscope from the FTC for the next 20 years. That is onerous. As well, fines may be applied immediately or upon failure to adhere to the order. So, if that periodic audit or the FTC looking into your program determines you have not maintained control and protection of sensitive personal data, you could be fined heavily.

Going back to the Wyndham Case, the list of security failures, noted by the FTC, was extensive. If you look at these things in today's light, you must wonder why were these even out there as issues? For example, storing credit card data in the clear. If you are PCI DSS compliant that shouldn't be. For example, applying simple passwords to control access to sensitive data. Today we use two-factor authentication if you need to get to that data. For example, failing to use firewalls and standard security technology. This speaks for itself. For example, failing to oversee the security of hotels that connected to Wyndham's servers and allowing vendors to have unnecessary access to the Wyndham servers. This is a very large problem we have with companies today when third parties either have unvetted access to corporate networks or poorly controlled access to corporate networks. For example, failing to take "reasonable measures" for security investigations or incident response. We might consider these things standard security practices today, but Wyndham chose to challenge the FTC's authority to enforce actions. The Third Circuit determined that unfairness provisions in Section 5 provided the FTC with the authority to regulate data security. The provisions of the enforcement action were supported by the Third Circuit court.

The LabMD case, however, is another interesting case of the challenge to the FTC's authority to regulate security. LabMD convinced federal trade administrative judge (ALJ) that his company's actions had not caused or likely would not cause substantial injury to consumers. There were two incidents. First, the third party they used released personal information from an aging report with about 9,000 people impacted. In the second incident, personal information including social security numbers was found in possession of an unauthorized individual. This was a much larger breach. The judge ruled that FTC had failed to demonstrate potential for substantial injury.

What had the FTC alleged in that case? They alleged that LabMD had failed to take adequate safeguards, failed to develop an information security program, didn't identify risks, had inadequate access controls to protect personal information from unauthorized personnel, lacked authentication security for remote access to their

network, lacked maintenance on operating systems, and failed to deploy "readily available" prevention and detection measures. You'd think that was a substantial list of failures. Despite these findings, the administrative law judge ruled that unreasonable data security "…caused or is likely to cause, substantial consumer injury". The importance of the administrative judge ruling is that the mere threat of identity theft after a data breach is not sufficient for a Section 5 claim. However, the full Federal Trade Commission reversed that administrative judge's ruling of dismissal of charges against LabMD. So, their enforcement action should have gone into effect. Their ruling of the full Federal Trade Commission stated that a demonstration of significant risk of injury is sufficient to meet Section 5's "likely to cause" requirement. Since personal information of millions of people was exposed this created a significant risk of injury and therefore satisfied the requirement. However, on June 6, 2018, the Eleventh Circuit raised issues regarding the FTC's power and practices.

If you go out to the lecture section, I have a link to a very detailed analysis of the ongoing FTC authority and the questions raised by the Eleventh Circuit Court.

Unit 1 – Part 2

In the second part of the lecture, I'd like to look at two documents that the FTC produced to help clarify the types of security practices that a company might put into place to protect personal information. The first of these was in 2011, called *Protecting Personal Information*. This was the first effort by the FTC to highlight how companies could secure their enterprises. It isn't too specific on the details and does not cite any FTC enforcement actions but is still valuable in the principles that it outlines. There are five principles in this first document. 1) **Take stock**. In general terms this means understand what you've gathered, i.e. credit card data, health care data, and where it is and how it is protected. Plan to protect that data. Think about establishing practices and procedures that will ensure that data is protected. 2) **Scale down**. It is a simple term. If you don't need it, don't keep it. For instance, if you have credit card data that you are finished using, don't save it. Now there are specific cases where we have recurring charges, then you do need to save the data, but there are ways to save the data in a protected format that doesn't compromise the underlying information. 3) **Lock it.** That means, simply, if you do have to save it, encrypt it. Protect it. Protect how you get to it. Segment your networks. Keep in mind the FTC wasn't this specific on how to protect the data, but in fact is saying lock it up. 4) **Pitch it.** Again, if you don't need it, throw it away. Really, this and scale down are two hand-in-hand items. 5) **Plan ahead**. Think about, as you develop new applications or new infrastructure in your company, how will that impact the data you are tasked to protect?

Since there was not a great deal of guidance in the 2011 pamphlet, the FTC put out a second document, called *Start with Security: A Guide for Business* in 2015. This was a reaction to FTC criticizing companies for not having adequate security when the FTC didn't have any standards they were using. Since they did not articulate any standards, they produced this pamphlet. Since this was a guide, it was not formally approved as a regulation, so it is not binding in court. But, the pamphlet does draw upon the facts of many of the FTC enforcement actions to help lay out the ten principles that they wanted to promote to companies in an effort to assist them in developing their cyber security programs.

Let's look at the first five principles in this pamphlet. 1) **Start with security**. If you're designing a new product, new application, new infrastructure, or whatever you're putting into place, think about security from the start. For instance, if you are developing an application, how will that application interact with secure data or personal information or protected data that you have. How will it interact with it? Start with that concept. Securing applications that look at personal information is a very difficult process, especially if you build security in after the application has been developed 2) **Control access to data sensibly**. Put in authentication controls, use two-factor authentication, make the process of accessing the data a reasonable but necessary method of protecting the data. For instance, segmenting

the networks helps. 3) **Require secure passwords and authentication**. Again, thinking back over several of the cases we've looked at, make your passwords strong passwords. Make the authentication mechanism a strong authentication mechanism, so that if somebody has to go from an unsecure network into a secure network, you are using that two-factor authentication. 4) **Store sensitive personal information securely and protect it during transmission.** Here's where you'll use TLS, and other mechanisms to protect the data in transit, but remember when it's stored (sitting at rest) it also needs to be protected. You'll want to make sure it is encrypted. However, make sure the encryption key is not easily accessible to people who don't have a need to access it. 5) **Segment your network and monitor who's trying to get in and out.** Keeping the network segmented allows you to put access controls in place, monitor your networks, and monitor your access control, so that you can see who is taking steps to try to get into your segmented networks.

The last five principles of that pamphlet: 6) **Secure remote access to your network**. I can't emphasize this one enough. Many breaches of companies are through the remote access to their network. It is an incredibly high percentage of companies that are breached in this manner. Look at your remote access and strongly tighten up the security on the remote access to prevent someone from unnecessarily gaining access to your network. 7) **Apply sound security practices when developing new products**. I spoke of this earlier. Make sure that you think about security practices when you are thinking about new products, new applications, and new infrastructure. Build those in from the start. Even though we have people who are very talented at testing the security of networks and applications, it is important that you think about secure coding techniques and secure application development techniques, and that they are built into the software development lifecycle as you move forward. 8) **Make sure your service providers implement reasonable security measures.** Again, a place where people tend to fall down is working with a third-party, but not really understanding how secure they are. A lot of times people simply say here is a security questionnaire, fill it out and let me know how secure you are. And, that is a step, but you want to go out and visit the companies occasionally and verify with your own eyes and ears that the security is as they claim it. 9) **Put procedures in place to keep your security current and address vulnerabilities that may arise.** Many people don't do enough vulnerability testing. Do vulnerability testing against your networks, your applications, and your infrastructure to make sure, where you do have exposed elements in your network, that those are tightened up through patching or something like a web application firewall, if necessary. Also do penetration testing. People confuse penetration testing and vulnerability testing. Penetration by a skilled penetration tester can show you how hackers might actually try to attack your network and get access to it. 10) **Secure paper, physical media, and devices.** This is an important aspect if, at any point in time, sensitive data is subjected to being put on paper. Make sure you have secure disposal capabilities of destroying the paper. Don't just wad it up and throw it in a

dumpster. For physical media-- before you throw a disc away or before discs are replaced or before you turn in a printer, which uses a hard disk as a means of storing data that is being printed-- make sure those disk drives are wiped forensically before they are released. Devices – make sure all your devices have up-to-date patching, and if they are used to store any type of sensitive data, that they are encrypted. Again, keep in mind that you need to wipe those disks before any of those devices are retired.

Unit 1 Part 3: Lessons from FTC Complaints

I will look at some lessons from FTC complaints. Few FTC enforcement actions actually end up in court. We looked at Wyndham and lab MD, and those are rather important exceptions to the norm. Most companies settle with the FTC and accept their conditions in the 20-year oversight, which is pretty onerous when you think about it. The companies might use the ten principles and start with security to really understand what the FTC might examine when they're looking at the security practices of a company. The company itself could actually reverse that and say here's the ten things that the FTC might be looking for. I want to make sure these are really nailed down tight. The lack of these measures might constitute unfair or deceptive trade practices in their eyes. Again, starting with security, these measures would provide sound security principles for developing a basic security program. There's much more that you want to do in developing that strong security program, but it's a good starting point if you have no program.

The FTC provides us another very good source of information as well. A lot can be learned through examining the representative cases of FTC enforcement actions. The FTC breaks these down into three general categories: 1) security of highly sensitive personal information 2) security of payment card information 3) security violations that contradict public policy. We'll see in later lectures where inadequate security practices by financial institutions are again challenged by the FTC and other organizations that are responsible for governing the protection of personal information inside of financial institutions. Additionally, the FTC brings actions regarding failures to protect customer privacy. In some cases, we may find a complaint incorporates failures of security and privacy practices - We get basically two different viewpoints on protecting the data.

What is sensitive information? The FTC doesn't really define sensitive information. However, they're more likely to bring action in cases where there's a failure to safeguard certain things, such as a health condition or some other personal trait, or there's likelihood of a disclosure leading to identity theft. Possibly social security numbers or credit card numbers are stolen. The long and short of it is the FTC expects companies to adopt industry standard practices, and to continue to enforce them within the company.

Now there are a number of cases in the textbook, and I want you to read all of them for several reasons. You will learn something from each case and that can help build a strong security practice when you're putting your security practice together. These cases might end up on a test or quiz sometime along the course. That possibility may also play into your strategy on reading those cases.

Schein Practice Solutions produces software for Dentist practices. If you think about lawyers, dentists, and doctors, they all have software that helps manage their practices. The software keeps track of patients, individuals that a lawyer may be working with, etc. The database engine used by Schein Practice Solutions was provided by a third-party. The database protected the data with an insecure proprietary algorithm and Schein Partners was made aware by the third-party that the algorithm did not meet industry standards.
They were notified by the US CERT that the database was protected by a weak

obfuscation algorithm. For those of you who aren't aware, weak obfuscation algorithm is simply an algorithm that hides the data. It keeps honest people honest, but it doesn't do much to protect against a talented hacker who wants access to the data. Schein Partners continued to claim that the product encrypted patient data, even after they were notified by US CERT that that wasn't the case. The key lesson here is if NIST or the US CERT tell you that your database is not protected by a strong encryption, then it's not protected by strong encryption! They are the experts in encryption. The FTC followed up after the company did not cease its claims of encrypting patient data.

In the case of the Matter of Reed Elsevier Inc. and Seisint Inc:
Reed Elsevier also reproduced a product called LexisNexis. For those of you who aren't aware, it is a database that stores information that lawyers can use to look up previous cases. It can also be used to look up data regarding individuals that they are working with on a case, or landlords can use it, debt collectors can use it, and employers can use it. It stores a lot of information such as credit reports, driving records, Social Security numbers, etc. To protect the data the company implemented safeguards. However, there still was a breach of over 300,000 individuals which occurred using a legitimate customer ID and password. How that customer ID and password was obtained, I don't know. It could have been by malware on the customer side, or through a breach of Reed Elsevier, or it could have been simply something that was shared by a customer of somebody else. However, the thieves used the information to open credit card accounts. Despite the company having some precautions implemented, the FTC brought action against the company.

The FTC alleged the breach was caused by company failure. They allowed common dictionary words as passwords and user IDs and customers could share credentials with each other. Users were not required to change passwords routinely, the number of unsuccessful attempts was not limited, and credentials were stored in cookies for customer convenience. Likewise, encryption of credentials or searches in transit were not required. Customers could create new credentials without confirming their identity. Think about that, if I log in with a customer ID and password, I could create other credentials without confirming my identity. That does not sound good. The company website was subject to common forms of attack.

The key lesson here is don't assume that password protection alone protects data. You must regularly assess the strength of authentication practices. This is why we see a lot of people, as I said earlier, using things like two-factor authentication to protect access to sensitive data. Ensure that malicious actors cannot bypass authentication safeguards. That's an important test that can be done by penetration testers, for instance, who are looking at your network.

In the matter of Eli Lilly and Company:

Lilly was a manufacturer of Prozac. They offered an email service called Medi-Messenger to remind patients of their medication. The company decided to terminate the service and blast emailed over 669 customers. However, it put the email addresses in the To line instead of the BCC line. Consequently, everybody who got the email could see everybody else's email addresses. Therefore, Lilly violated the privacy of some of those individuals. The FTC alleged that Lilly failed to adequately train individuals handling sensitive information.

The key lesson is that the FTC will hold a company liable for the actions of one employee. It's very important that you train individuals who must handle highly sensitive data to understand what their responsibilities and their liabilities are in working with that data. The FTC in this case differentiated sensitive from non-sensitive information, but again held Lilly responsible for the fact it had released that information to a large number of individuals.

The second focus of the FTC is a failure to secure payment card data. There are many cases of breaches over the last decade. There's a plethora of cases to look at regarding the failure to secure payment card data. Even with the advent of the payment card industry data security standard, the PCI DSS as it's known, breaches continue to occur. There's been some very notable cases lately: Target, Heartland Payment Systems, and Home Depot. Why do they continue to occur?

Let's look at the case of Guess. They had an e-commerce site which was compromised by SQL Injection attack. This case was in 2003 and by then SQL Injection was several years old. That's something you ought to look at. Look at SQL Injection because it's still a successful attack today. It's roughly on its 20th year, give or take, maybe more. I'd have to go back and look at when they the first one actually occurred. Hackers were able to access customer credit card information. The FTC cited that Guess stored credit card data in clear, unencrypted and in readable text. This was against the company policy, but they did it anyway. FTC alleged the company failed to detect reasonably foreseeable vulnerabilities in their website application. They also failed to prevent visitors to the website from exploiting those vulnerabilities. There are very simple tests to test an application, particularly a web-based application, on whether or not it can be subjected to various types of injection attacks. So, it's that testing that wasn't done by Guess and should have been done to prevent this. The key lesson is any claims of adhering to PCI DSS standards must be strictly followed and that includes being able to secure your applications and the way they access sensitive data.

In the Matter of Petco Animal Supplies, Inc.:

In 2004, Petco Animal Supplies operated Petco.com which had direct sales to customers. The privacy policy stated that entering credit data was completely safe and encrypted. In 2003, a hacker used SQL injection, again, to obtain complete credit card information. The FTC determined that Petco did encrypt the data in transmission to their servers, but it was subsequently stored in clear text. The FTC alleged that Petco did not implement reasonable and appropriate measures to protect personal information against unauthorized access. The important thing here is to remember you have to protect credit card data in transmission, in processing, and at rest in storage. That's the key lesson that the text highlighted.

In the Matter of Dave & Buster's:

The facts were that Dave & Busters operated 50 indoor entertainment centers nationwide. They experienced a breach of 130,000 customer payment card numbers. Hackers installed unauthorized software on the company networks, which enabled them to capture card data as it was being sent to the card processing service provider. When a company like Dave & Buster's takes a credit card, that data is stored, and then at night, it's sent up to the credit card processor. That company is responsible for notifying the various banks and etc. and helping to get the money back to Dave & Buster's, and at the same time crediting the card account of the individual who made the payment.

The FTC alleged that Dave & Buster's failed to adequately detect unauthorized access to their networks and to monitor third-party access. The key lesson is companies should routinely audit their systems to ensure no unauthorized software has been installed by a third party. There are some very good security tools for doing this, including whitelisting of applications that can run on your network.

Unit 1 Part 4: Lessons from FTC Complaints

The third category highlighted by FTC was the failure to adhere to its security claims. Sensitive information is a strong focus of the FTC, even though they don't really provide us a definition of sensitive information. However, non-sensitive information can also hit their radar. It could be true if a company's privacy policy, marketing materials, or public claims that they make attest to the fact that they are protecting data. If a company fails to meet its claims, they may meet the FTC. The FTC expects companies to adhere to their claims on cyber security and will pursue those who don't. The FTC may interpret the company's claims and marketing material broadly. Think about this, a statement that you may make in your marketing material, which is fairly innocuous but implies certain protection of data, may be interpreted fairly broadly by the FTC and could hold you to those claims that you are protecting your data in a secure manner.

Let's look at a few cases:

In the Matter of MTS Inc. doing businesses as Tower Records/ Books/Video and Tower Direct, and TowerRecords.com.

The company operated TowerRecords.com, which claimed to use state-of-the-art techniques to safeguard personal information. It also claimed to protect sensitive data in accordance with the Terms of Service and Privacy Policy. However, the checkout functions were redesigned at some point in time, and thus created a vulnerability that allowed a customer to enter any order number and view other customer's data. The FTC alleged that more than 5,000 customers' purchased data were accessed. The FTC attributed the vulnerability to failure to implement checks and controls on rewriting and revising the application. The FTC alleged that there was a failure to implement appropriate security tests and inadequate training on identifying web application vulnerabilities and security testing. Keep in mind, there is software available to test application security and companies that specialize in testing application security that could have helped in this case. If it's done by people inside the company, they need to be trained on being able to identify those vulnerabilities and testing the security of applications. More importantly, this whole process needs to be part of the SDLC so that, as applications are redeveloped or modified, this testing becomes automatic in the process. The key lesson is a general promise to protect customer information sets an expectation with the FTC, and failure to adopt safeguards will attract the attention of the FTC.

In the Matter of Oracle Corporation:

Oracle produces Java software which is used at many devices and in many applications. Periodically, Oracle releases updates to the software to eliminate vulnerabilities. Oracle made claims that Java provides safe and secure access to the world of amazing Java content. Even with the update, the older vulnerable versions however were left on the computer. The FTC noted that leaving the older versions on a computer might subject users to serious well-known attacks. Think about it, the new version which was patched was on the system, but the old versions which had the vulnerabilities that could expose the computer to be compromised were left on the systems as well. The key lesson is if a company is aware of a major security vulnerability that could expose customer data, it should disclose that vulnerability and the ways to fix it.

In the Matter of Credit Karma Inc.:

The facts are Credit Karma provided a mobile application that allows customers to view their credit reports and scores. If you haven't used this application, it's actually a very interesting application and allows you to do just that. The company privacy policies claim that it uses SSL to establish a secure connection. Apple devices, iOS, however, provides a programming interface that by default uses SSL. Apple warned developers that disabling the default settings might impact the secure connection. Sure enough, Credit Karma overrode the default settings and therefore did not use an SSL connection. This opened up Credit Karma to redirection interception attacks. The FTC further alleged that this presented a potential that a user's credentials might be compromised. This could expose a user's credit report and financial data as well. They also asserted that misuse of this data could lead to identity theft.
The key lesson is that the FTC has addressed several cases where companies have modified default settings that impacted underlying security of data. FTC has a very low tolerance for companies that do this. The default settings are becoming the de facto standard of mobile application development and should remain in place.

There are a number of cases in the text that address various viewpoints of the FTC. The cases cited here are not meant to slight any company or suggest avoidance of their services or products, by any means. The important lesson is to learn from these companies' failures. The last thing you want to become is subject of an FTC enforcement action. Understand what claims you're making and whether you can back them up. Understand that FTC may interpret your statements broadly and that you need to implement reasonably secure practices to protect your user data.

Unit 1 Part 5: State Data Breach Notification Laws

We've noted that there's no federally mandated security standard in several places within the unit, to-date. The FTC has stepped up to fill this void using Section 5 of the FTC Act, but, with a lab MDK still at issue, the future of FTC enforcement actions may be at risk. Forty-seven states and the District of Columbia have individual mandates for breach notifications. These require companies and government agencies, upon breaches, to report to consumers, regulators, and credit bureaus.

These laws are very important to your security strategy because you have to understand how these state laws will impact you should you have a breach. You need to understand a number of different things if a breach occurs. For instance, a burglary takes place in one of your offices in California, computers are stolen, and you are informed that sensitive data was stored on them. What type of data was stored on the computers? How many records were stolen? Did all of the data pertain to just California residents or were users in other states impacted? What are your disclosure requirements? You have to understand all of these elements if a breach occurs and you have to understand them fairly quickly. Knowing what to do and what to ask ahead of time is very important.

Keep in mind that you don't have to have servers or employees in a state for the state law to apply. It's all about the data. If it pertains to a user in a particular state, that state's laws apply. The relevant state laws will determine whether and how a company must disclose information about a breach, how must you provide notice of the breach, and how you must inform the credit bureaus, regulators, and the consumers. Keep in mind that the states' laws in many cases look very similar, but there may be important differences, and it's important to understand those differences. Some of them may differ in how they define sensitive personal data. Some may differ in when regulators may need to be informed.

A very important consideration is that companies have contravening goals that they have to accomplish. On one hand, you're required to disclose the breach within time frames established under the state data breach laws. On the other hand, you have to understand the breach, what's the extent, the type of data compromised, and whether any sensitive data was compromised, as well as to manage the delays imposed by law enforcement. Inaccurate disclosure can subject a company to additional penalties under the state regulators.

Data breaches may not require disclosure. However, if the data are encrypted, in every state, except Tennessee, no disclosure is required if the decryption key was not available. It's important to understand any exceptions available under the prevailing state laws, because those exceptions may apply to the case that you have before you. Then, even if it doesn't, if you don't have sensitive data, will a company choose to notify consumers anyway? Well, that may be the case. Are breach notifications good business if no personal data were compromised? Is transparency a fundamental principle of the company? Those are questions you have to ask. Even if notification

only has to occur in one state, the news will make its way to the internet and to journalists.

State data breach laws only apply to unauthorized acquisition of personal data. This is defined by each state's data breach laws. If the compromised data don't meet the definition of personal information, then a company doesn't have to disclose the compromise. However, in every state, there are minimum types of personal information data that have to be reported, if you have to disclose a breach. In almost every case, it's a first name or first initial and last name and at least one other category of data, such as a social security number, a driver's license, or state identification number, an account number, such as a credit card or bank account, or debit card number and any passwords or codes that are necessary to get into the account.

Additional personal information include: medical information, health insurance information; online account information such as biometric data, taxpayer identification numbers, tribal and identification numbers, any federal or state identification number, or date of birth.

More personal information includes: the mother's maiden name, employment identification number, passport number, digital signature, and, even in the state of California, the zip code of an individual.

California and Florida require notification, even if the consumer's name was not compromised. Instead of first name and/or initial and last name, it also could be username or email address, with a password, or a security question that is necessary to use that account.

As stated earlier, Tennessee is the only state that doesn't provide an exception for encrypted data. An issue might be the technical specifications for encryption. However, for instance, Massachusetts requires 128-bit encryption and the other states don't specify. It's important that most states require the decryption key not be accessed.

Two issues face the security people in the course of a breach: can we prove that the encryption we were using is sufficient to protect the data, and can we prove that the decryption key was not accessed? Another issue that could face security personnel is if you're subject to PCI DSS and credit card data is impacted, the decryption key cannot be anywhere on your network. For those of you who work with encrypted data, that poses some very interesting problems in being able to process your data.

The risk of harm is a very interesting concept. In thirty-eight states, notification can be avoided if it can be determined that there is no risk of harm for individuals. In Tennessee, for instance, this is the only exception to the encryption rule. Each state varies in its concept of risk of harm--this goes back to understanding how each state's data breach laws might impact your security operation. In Michigan, companies aren't required to notify individuals if they determine that security breach is not likely to cause substantial loss or injury or identify theft. That would be the

scale for risk of harm. In New York, notification exception applies if the company determines that the breach that did not compromise the security, confidentiality or integrity of personal information. That's a fairly broad statement on how to protect data.

Most state notification laws require companies to notify customers as expediently as possible without unreasonable delay, and the wording varies by state. You have to understand how those notification laws will impact your operation if there is a breach. Even without clearly defined timing, state regulators will not tolerate unreasonable delays. Eight states actually provide a specific time period. Florida within 30 days; Ohio, Rhode Island, Tennessee, Washington, Wisconsin, and Vermont within 45 days; and Connecticut 90 days. All states allow companies to delay notification if notification would harm a law enforcement investigation.

The form of notice this notification has to take is defined by each of the states. You must deliver notice, in the medium that's approved by the state law, to where that data is from. All states allow written notification to the last known address of an individual. Most also allow email to the last known email address. Some states only allow email notification if email was the primary method of communications. In about half of the states, notification is allowed by telephone, and in a handful of states, by fax machine.

There is a concept of substitute notice also, because in most cases you don't know either the last known address or the email address of a compromised individual. A substitute notice is used when you don't have sufficient contact information, or if the total cost of notification would exceed the amount specified by the statute, or the company would be required to notify more than a specified number of people. In some places, the state law may say if there are over 500 impacted records you can use a substitute notice. This generally consists of three elements: you can email the notice to any individuals for whom the company has an email address; you can use a conspicuous notice about the breach on the website, if the company has a website; or you can notify a major statewide media. Occasionally, you'll see these notifications in the newspaper ads in various big cities.

Most states do not require breach notice to contain specific information. However, a minority of states require very specific statements about the data, such as contact information for the company, general description of the breach, categories of personal information compromised, the dates of the breach, contact information for major credit bureaus, the state attorney in the FTC, and advice to remain vigilant about identity theft by reviewing your credit reports, and information about identity theft protection systems. Even if you're reporting to a state that doesn't have specific information designated, these are the elements that you would want to put in that notification.

Thirty-one states also take reasonable steps to dispose of records that contain personal information, such as shredding paper records, rendering personal information unreadable or undecipherable, or preventing the information from being reconstituted.

We've already talked about that if you have disk drives, you'll want to wipe the data on the disk drives; if the information is on paper, either shred, burn or put it into a liquid to dissolve it. You want to make sure that data is rendered unreadable. Most state statutes do not define what reasonable measures meet the letter of state disposal laws. There are a lot of third-party companies that can be used to dispose of records. You want to validate the operational controls of that third-party, get references, and review the security practices and policies to ensure that they securely handle any of the records that they're destroying and that they are actually destroyed. In many cases you also can ask for a certification that they have destroyed the data.

Final thoughts for Unit 1. We've had a lot of things to consider with respect to the legal foundations around collecting and protecting sensitive personal information. We looked at the FTC and use of Section 5, the FTC Act, and how the FTC has assumed authority to enforce data security throughout through its enforcement actions. We also looked at how the various states have implemented data breach laws governing a company's actions should it be breached. All of this information is important for the leaders of a security operation. When I was the chief security officer at a company, we constantly looked at all of this information, especially, as state laws changed, so that we would understand how that the change in a state law would impact our operation. If a breach occurs, that is the worst time to start planning on how to respond. Incident response and interaction with a legal group must be determined long before it is needed.

Unit 2 Part 1: Cybersecurity Litigation

Welcome to Unit 2:

If you look at the title Cybersecurity Litigation, you might say to yourself, why do I need to understand how to sue people? It's important to know what happens when your company is a party to a legal action. Legal processes have several procedural steps that take place and they're defined by either federal law or state law as to how they will proceed. As a security leader, and you will at some point in your career be involved in one of those stages. It's important that you understand what those legal processes are. We'll look at the legal processes in the federal court system, and we'll look at the processes in the state courts, and these vary by state. You're going to hear that a lot in this course, how it varies by state, because the definitions of common laws are defined at the state level.

A civil procedure starts with filing a complaint. This is a short plain statement by the plaintiff. A plaintiff is the person who is filing a legal action, or as we might say, "suing somebody". This complaint describes the defendant's actions and has to show that there's a violation of common law or statute. Common law is defined by judicial decisions or case law, for instance negligence or breach of contract. We'll look further at both of these in this unit. A statute is a law passed by a legislative body, an administrator board, or the municipal court. An example of this is the State Consumer Protection laws. There are a lot of other statutes that you're probably aware of, depending on your particular company and what your company does.

A defendant can file a motion to dismiss. A motion to dismiss is a written application to a court asking for a ruling. It argues to dismiss the case due to either a settlement, or a voluntary withdrawal, or a procedural defect. Think about it, if the plaintiff files the legal action, the defendant then can file a motion for dismissal. The defendant may not succeed at the motion for dismissal if the judge accepts the facts of the plaintiff. The defendant doesn't really get an opportunity to produce any evidence to present to the judge, at this point, in the legal proceedings. More than likely that motion to dismiss is probably not going to succeed.

That leads into what is called Discovery. Both parties have an opportunity to request information from the other party. This is compulsory and this could comprise interrogatories, written questions, or depositions. A deposition is out of court testimony converted to a written form. If you've watched any legal TV shows, you'll see depositions being made with the person sworn in by an officer of the court. They are giving testimony as if they were at trial, but it's done out of court. There could be requests for admission, which is a written factual statement. There could be requests for production, which is an inspection and copying some information that the other opposing counsel may have, it could be documents, or any other kind of tangible items. There are exceptions available for each party given proper procedures are followed. In general, discovery follows one of these patterns. We'll talk about how to protect against discovery to a point when we get a little bit further into the unit.

After discovery, either party may file a motion for summary judgment. This is where you present evidence gathered in discovery to the judge, you argue that even if that evidence was viewed in the most favorable light for the opposing party (in other words you give your opposing party the benefit of the doubt), no reasonable jury would find in favor of the opponent. The opponent has an opportunity to present evidence that counters those facts, and the judge decides to accept the motion or move to trial. Typically, in breach cases, the defendant is the one who moves for a motion to dismiss, and quite often never gets to the trial portion in a data breach case. In most cases a settlement is reached at this point in the process.

There are a number of other types of motions that can be filed during the pre-trial process. I invite you to look through some reference material if you'd like to see some of the other motions that can be filed. The defendants often face multiple legal actions. When you see data breach cases you usually don't see one lawsuit being filed, often you see a number of them. Some will be class-action lawsuits, some will be individual lawsuits, and you may see companies filing against the breached party. There'll be a number of different lawsuits that you'll see in the case of a data breach. Even class-action lawsuits have their own processes, and we'll look at those more in depth. They proceed much like the process that we've already looked at in a normal class action, an individual class action, or a company filing lawsuit against another company. But there has to be a process called Class Certification and we'll talk about what that means. There are four prerequisites that we have to beat before we can file a class-action lawsuit. We'll talk about those shortly.

Unit 2, Part 2: Article III Standing

A particularly difficult concept to understand in the legal process is called Standing or Article 3 Standing. Before a party can sue, it must be determined if they have Standing to pursue the case. Is the party bringing the legal action the proper party to bring such action? They must allege a personal injury traceable to the defendants allegedly unlawful conduct. In other words, you have to show unequivocally (in a way that leaves no dount) that the injury you suffered is traceable to an action that the defendant allegedly performed. It's likely to be redressed by the requested relief. Redress means that the relief you could be awarded for success in the trial will remedy the injury that you suffered. So, there are three separate prongs that have to be proven for standing: the plaintiff has suffered an injury; in fact, the injury is fairly traceable to the defendant's unlawful conduct; and the term redressability—and, as we said, it is likely that the requested relief will remedy the injury suffered.

There are two important cases to look at, and the book brings both of them to light in Spokeo v. Robins. Spokeo had a website with personal information about people. Someone accessed Robins' information on that site, but the site profile contained incorrect information, i.e. family status, age, employment status, education, etc. They had that incorrect information. Robins filed a class-action lawsuit alleging violation of the Fair Credit Reporting Act (FCRA). The FCRA requires reporting agencies to follow reasonable procedures to ensure the accuracy of their reporting. You've seen this several times with some of the other reporting agencies that are out there today. You have to limit the use of that information and those reports for employment purposes. In other words, you have to be very careful about using the information of those reporting agencies if you're using that information for making a hiring decision. Spokeo moved for dismissal stating that Robins did not allege an Injury-in-fact, and that it was just procedurally something had happened and the information was incorrect. The District Court granted the motion, but the US Court of Appeals reversed the decision stating that Robins had indeed alleged that Spokeo had violated his rights.

The Supreme Court sent the case back to a lower court concluding that the appellate court did not apply the proper test for Standing. The injury-in-fact must be concrete and particularized, and actual or eminent. so the Supreme Court stated that the complaint was particularized. His rights were violated and it's very particularized. For an injury to be concrete it must actually exist. It doesn't have to be tangible, but it cannot simply be a procedural violation without further indication of harm. To argue that it was just a procedural violation did not make the injury less concrete. This was remanded back to the Ninth Circuit to analyze whether Robins' Free Credit Reporting Act (FRCA) rights were sufficiently concrete.

In Clapper v. Amnesty International USA, a group of attorneys, media organizations, labor groups, and others who communicated overseas filed a lawsuit challenging the Federal Intelligence Surveillance ACT (FISA). That issue was the requirement that plaintiffs allege an injury-in-fact was allegedly traceable to the FISA program. In other words, these are people who communicated overseas regularly and they felt that

their injury was traceable to the FISA program itself. They didn't argue that the government intercepted the communications of these individuals, but rather that there was a “reasonable likelihood” that the government might obtain their communications at some point in time. The risk was so great that the communicants were forced to take costly and burdensome measures to protect confidentiality of international communications. The harm was actually two-fold that their communications at some point in time might be obtained, and secondly that they had to spend a large amount of money and effort to protect their communications. However, the Supreme Court rejected the plaintiffs’ arguments. First of all, they said it was a speculative chain of possibilities of injury. For instance, it's a reasonable likelihood that the whole chain of events would have to happen for that injury-in-fact to be real. The second argument also failed as it was based on the cost incurred on that speculation of future injuries. The Supreme Court rejected the plaintiffs’ arguments.

Injury-in-fact can be a significant hurdle in most data breach lawsuits. There are both broad and narrow views of how to look at harm. In Krottner v. Starbucks, there was a broad view of looking at injury. In this case Starbucks had a computer with data on 100,000 current and past employees that was stolen. It contained names, addresses, and social security numbers. Three employees filed a class-action lawsuit alleging negligence and breach of implied contract. The first claimant claimed that she spent a substantial amount of time monitoring banking and retirement accounts. The second claimant had basically the same claim. The third was alerted by his bank of a third party’s attempt to open a bank account with his social security number. The Ninth Circuit ruled in favor of the plaintiffs arguing that they had alleged a credible threat of real and immediate harm. Compare that back to the previous case we looked at. You can see in this case there really was a threat of real and immediate harm, because their data had been stolen and could have been used. In the third individual’s case, it actually had been used in detriment to the individual. The Krottner case made it easier for data breach plaintiffs to establish Standing in the Ninth Circuit.

Reilly v. Ceridian Corp. presented a narrow view. This was filed against the payroll company Ceridian after a data breach exposed data of 27,000 people. However, there was no evidence that the hacker ever read or copied the breached information. The district court granted Ceridian’s motion to dismiss for lack of Standing, and reason that hypothetical harm, again no real harm, actually had been presented. There was only theoretical harm and nothing more to establish an injury-in-fact. A harm has to be fairly traceable. Remember we said that for it to be in Standing it had to be fairly traceable back to the actions of the defendant. After considering an injury-in-fact, you must show that the injury was fairly traceable to the defendant’s failure to adopt data security practices. In Resnick v. AvMed Inc., they had social security numbers on a stolen laptop. The stolen laptop had data on it, and if the data were used to create identity theft, you have a fairly traceable act.

Refer back to redressability--remember redressability means if a remedy is proposed by the court it will take care of the injury or cover the injury that was suffered by the plaintiff. This is the final prong to prove in Standing. It's easy to establish in Resnick v. AvMed Inc.: the plaintiff suffered monetary loss as a result of a breach. The award

of compensatory damages would redress that injury. There have to be quantifiable damages if you want to have an easier path to prove redressability. If your or your company is the victim of a data breach it's very important to keep track of all those expenses that you incur. Also, keep track of your time spent. For instance, if you're having to track down with your bank, on a repeated basis, whether or not somebody is trying to steal something out of your bank account, identity theft, or monitoring your credit reports etc. That's important if a lawsuit ever takes place so that you can indeed show both injury, traceability, and redressability.

Unit 2, Part 3: Common Causes of Actions

There are several common causes of actions in legal proceedings. Negligence is probably one of the most common and I'll look at this in more depth a little bit further into this unit. Breach of contract is one that you'll see fairly often, so that's another one I want to cover more in depth. All of these are covered in the book in a fair amount of detail. You really should read all through all of these because they're very important to understand, and again may show up on a test or quiz later. To prove negligence there has to be a Duty owed to the plaintiff and that the Duty was breached and caused an injury to the plaintiff. We'll look at this in a little bit more depth. Negligent misrepresentation is when you have a defendant who failed to exercise reasonable care and supplied false information causing a plaintiff to suffer a pecuniary loss. Look at Reasonable Care and Reasonable Duty. You'll see these terms in a lot of the different laws that relate to an interaction between two parties. It is interesting to try to understand what "reasonable" means in these cases. Breach of contract is when the defendant breached a contract with the plaintiff. In a breach of implied warranty, the defendant's product or services failed to satisfy basic expectations of fitness.

Invasion of privacy and publication of private facts are the publication of private facts that were offensive and not of public concern. Unjust enrichment is when the defendant knowingly obtains a benefit from a plaintiff in a manner that is unfair. It is inequitable for the defendant to retain the benefit without paying for it. For instance, I may have tried to buy something from you, but I lied about its providence. I ended up buying it from you for a very small amount of money, or worse, let's say I tried to sell you something that had an invalid provenance and I took the money from it. There's a number of different ways that you can look at unjust enrichment. In state consumer protection laws the defendant's conduct can constitute an unfair competition through unconscionable acts that were unfair or deceptive acts of trade or commerce.

Let's look at negligence in a little more depth. This is one of the more common causes of data breach related lawsuits, and it's a common law tort. There are precise rules that are developed through court rulings, and, unfortunately, they vary from state to state. There have to be four elements that are proven for there to be negligence. The defendant owed a legal duty to the plaintiff; the defendant breached that duty; the defendant's breach caused cognizable injury to the plaintiff (cognizable is just that it's something that you can see, feel, or touch); it's an injury that can be observed. The first two elements typically are not subject to much dispute in data breach litigation. You owed a duty to the plaintiff; the defendant breached that duty. In data breach scenario, it's pretty simple: you had card data; you were hacked; card data was stolen. You had that legal duty to protect that card data; it was breached; the card data was stolen; you breached your duty to protect that card data.

The legal duty is supported not only by state law but also common sense. For instance, if you're collecting credit card data, that imposes a legal duty to protect that data. The compliance with the PCI DSS is mandated by the card networks. If you have card data, you have to be compliant at all times with the PCI DSS, and this is hard to do. Companies change networks; companies move data around; and/or they

do a number of different things that may expose that data. Common sense suggests that a company would do whatever it takes to protect that data. That means you have to start thinking about security when you're designing new networks, writing new applications, or whatever. You have to understand what might happen to that data, which you have a duty to protect. The defendants claim they are hacked by a third-party. Therefore, they didn't breach a duty of care. They were hacked. This is generally rejected by the courts. Courts reason that a company played a key role in allowing the hack to occur because they didn't protect the data. They had the data for some reason, in a way that it could be reached, and hacked by a hacker. Therefore, the company was a participant in allowing that hack to occur.

The courts use the following factors in determining if a duty exists:

- That there is a foreseeability of harm to the plaintiff--if you're holding card data you should probably see that stolen card data could harm a plaintiff;
- That there is a connection between the defendant's conduct and the injury suffered;
- That there is moral blame attached to a defendant's conduct--in other words, if one just really didn't care about the data or didn't patch my systems, then, there's probably moral blame there.
- Is there a policy for preventing future harm;
- A burden is imposed on the defendant and community to impose a duty to exercise care with the resulting liability for a breach.

Cognizable injury is the largest barrier to the plaintiffs. Demonstrating a breach of legal duty causes a cognizable. State courts have worked out how to determine if injuries occurred and the plaintiff, quite frankly, can be successful in some cases, and not so in others. Again, it may vary by state.

Often, they apply what's called an Economic Loss Doctrine. It is the principle that a plaintiff generally cannot recover from financial harm that results from injury to the property of another. There are two primary differences among the various versions of Electronic Loss Doctrine. Some states recognize that there's an independent duty exception to the doctrine. Other states recognize an exception of the doctrine where there's a special relationship between the plaintiff and the defendant. It's not so much that you understand those two differences, as much as it is just to understand that a cognizable injury has to occur and there are some exceptions that may be applied at the state level, based upon how they look at the Economic Loss Doctrine. The plaintiff suing for data breaches or inadequate data security faces his best chance in negligence claims, because you can demonstrate actual harm resulting from poor data security.

Causation is another thing that has to be proven in negligence. The plaintiff still has to demonstrate that the breach of duty caused the injury. The defendant must link the inadequate data security to the identity theft or other harm. This sometimes is very difficult to prove. However, the courts are willing to make reasonable assumptions. For instance, all social security numbers are stolen from "Company A", and, immediately thereafter, identity theft starts hitting our credit cards, bank

accounts, etc. That's probably a clear indication of the two things being connected. However, we can't really show that the hacking of “Company A” actually resulted in the identity theft that occurred immediately afterwards. Causation is easier to prove if the duration from the breach to the identity theft is short. So again, if it happens right after the breach takes place, you're probably going to be successful in getting a little leeway on what that reasonable assumption is. If it happens six months later, or a year later, or doesn't happen till the next year, it's going to be most difficult to prove that link between the breach and the harm.

Breach of Contract is another common claim by plaintiffs. Precise elements of Breach of Contract vary by state and the contracts are laws that are set by common law. However, most of the contract laws at the state level are created through adoption of what's called the Uniform Commercial Code, so they're fairly similar. The plaintiff has to show that there actually exists a contract between the plaintiff and the defendant, that a defendant's breach of a duty was imposed by that contract, and that damage was caused to the plaintiff as a result of the breach. A contract often has data security provisions where I might say to “Company A”, you must protect my credit card data by being compliant with the latest version the PCI DSS, at all times. Then, if a breach occurs, I have a contract provision which may allow me to pursue a lawsuit under breach of contract. By the way, I might also be able to pursue it under negligence, as well, and it may be much easier for me to prove harm.

Breach of Contract. There are three primary methods that a plaintiff could attempt to bring a breach of contract rising from a data breach of poor data security. You could sue for the breach of an expressed contract to provide a specified level of data security, and that's the most likely route for success. This is what I was talking about earlier with that provision in my contract for data security. You could claim that you were an intended third-party beneficiary of a contract between the defendant, and another party, in which the defendant agreed to provide a certain level of data security. This is a little more tough to prove that you were actually an intended third-party beneficiary of a contract. This might be the case, for instance, where a company that has your credit card data actually has it stored someplace else on another system with a third-party. That party is hacked, or the company is hacked, and your data is stolen. The plaintiff could claim that even though there was not an express contract with the defendant, you're still covered. So, the parties had an implied contract. The defendant agreed to provide reasonable level of security, and, therefore, you can argue that you were harmed under the breach of an implied contract.

Unit 2, Part 4: Class-Action Certification

Class-action lawsuits require what's known as Certification. Even if a plaintiff succeeds in demonstrating Standing, and that they have stated a sufficient common law or statutory claim, they face an additional hurdle which is called Class Certification. Why are class-action suits filed instead of individual suits? Well, think about it. If I have a lawsuit that might result in $500 worth of harm, the remedy of $500 is not really rewarding to my attorneys. They're only going to get about a third of it and the expenses of the lawsuit probably are going to exceed what we're going to get. On the other hand, if I have 100,000 other class members all getting $500, then that certainly covers the attorney's fees, as well as the expenses much more comfortably. It allows us to get all of the class members together and show some of these other points, that we'll talk about shortly, in the case rather than just me as an individual. Class actions typically will begin with a small group of plaintiffs called class representatives. They file the class action complaint on behalf of the entire class of affected individuals. A successful verdict on trial would be divided among all the members of the class, or, if we decide to settle before we go to court, then the settlement is divided among the members of the class.

Plaintiffs can't automatically feel entitled to receive the damages or settle on behalf of the class. That class must be certified first, before they can they can do that. It's easier to bring class-action litigation into a Federal Court. The plaintiffs must convince a judge that they satisfy Rules of Civil Procedure 23, and that is divided into two parts, 23(a) and 23(b).

23(a) has four prerequisites. There has to be numerosity--the class is so numerous that the joinder of all class class-members is impracticable. In other words, there are so many members that are represented by the class, that to have them all come together at one trial would be impossible. There has to be commonality--questions of law or fact are common to the entire class. If we were filing negligence and breach of contract, then all members of the class would be filing that same cause of action. There has to be typicality--the claims or defenses of the representative parties are typical of claims or defenses of the class. There has to be adequacy--the representative parties will fairly and adequately protect interests of the class. This generally involves the attorneys experienced at class-action lawsuits. They fairly ensure that the monies are distributed among the members of the class and the class representatives are not in conflict of interest with the class itself, etc.

The biggest hurdle in this case is proving commonality. In the Walmart v. Dukes case, there was a massive class action lawsuit representing 1.5 million female Walmart employees. The Supreme Court ruled that three plaintiffs did not satisfy the commonality requirement. The case argued that Walmart's corporate, and not a corporate policy, led to the discrimination against female employees. Understand that there wasn't a corporate policy that said discriminate against women. It was the corporate culture and local supervisors that had discretion over pay and promotion. You could say that it wasn't Walmart that was discriminating, it was this culprit corporate culture implemented by local supervisors that had discretion over paid

promotion that was the inequity. This was not enough to demonstrate commonality. Therefore, they couldn't go forward with the class-action lawsuit.

Class representatives must show that their case falls into one of four categories. These are the four categories of 23(b):
Numerosity: Separate claims would possibly create inconsistent or varying adjudications. In other words, if all 1.5 million female employees of Walmart filed individual claims against Walmart, there would be probably 1.5 million different adjudications of those claims. Some might be successful, and some might not; some might get a lot of money and some might not. Separate claims would be dispositive of the interests of the other members not party to the individual adjudications and could impede their ability to protect their interests. The goal is declaratory or injunctive relief. They were filing an injunction to stop some type of action. If questions of law or fact common to class members predominate, class action is superior to other available methods.

The Hannaford Brothers Company Customer Data Security Breach litigation is a putative class action lawsuit. Putative means reputed, believed, or supposed by most people. The class representatives brought seven claims, five of which were dismissed, but look went forward. Negligence and breach of contract were allowed to proceed. The district court concluded that the plaintiffs satisfied Rule 23(a). In numerosity there were thousands of card holders that purchased identity theft protection and thousands were charged with replacement card fees. It was impossible to determine if Hannaford breach was the proximate cause of the expenses, but the court was permitted to draw reasonable inferences about that numerosity. They felt numerosity was met.

Commonality: the losses may vary by individual class members, but the claims arise from the common question of whether Hannaford's actions caused the breach.

Typicality: the class representatives and members of the class are aligned, thereby demonstrating that Hannaford was negligent and the breach of an implied contract took place. Hannaford argued that the economic harm to the class members varied, which it probably did. The judge determined that the varied actions by the class members was a mitigation to alleged actions of Hannaford itself.

Adequacy: in the Hannaford case, the class representatives had to demonstrate that there was no potential conflict between the representatives and the class members. The lawyers were qualified, experienced, and able to conduct the litigation. So, adequacy was met. The class representatives chose a lawsuit rather than accepting gift cards from the company in terms of refund, but the judge ruled this was not a conflict of interest in the case of class representatives. Thus, all four prerequisites of the class were met under 23(b) and it proceeded.

In the Heartland Payment Systems Customer Data Security Breach, litigation suffered a breach of a 100 million customers payment card data to hackers. A number of consumer lawsuits were filed across the nation. As I said earlier, usually you don't see just one suit in a data breach, normally you will see multiple lawsuits filed against the company that was breached. This was consolidated into one case in Texas, and the parties reached a settlement. The judge concluded that the plaintiffs met all four requirements of Rule 23(b); Numerosity with 100 million member class; Commonality, the common factual question was what did Heartland do before, during, and after the breach to safeguard consumer plaintiffs' financial information?; Typicality, the outcome of the claims center on Heartland's conduct, not any member, so it was on all of the individual members of the class. It was a breach by Heartland that affected all of them; Adequacy, plaintiff's lawyers were experienced and there were no conflicts with class representatives. Therefore, all the provisions of Part 23(b) had been met and the settlement proceeded.

Unit 2, Part 5: Cyber Insurance

The last two elements that I'd like to look at in this unit are Cyber Insurance and work product protection. Settlements and adverse verdicts from trials can be very costly to a company. Many companies look to cyber insurance as one means of covering those costs. It could be general liability insurance, riders covering cyber events, errors and omissions insurance, or specialized policies covering cyber events. Insurers may go to court to challenge companies attempts to get coverage for data security breaches under their policies. They're divided over a point called publication.

Some courts conclude that any data breach constitutes publication of personal information and should be covered under commercial general liability policies. This brings up the case of Travelers Indemnity Company of America v. Portal Healthcare Solutions. The customers filed a class action lawsuit against Portal, a healthcare company. Portal had been breached and exposed medical records. Travelers, its commercial general liability carrier argued that exposure of the data was not a publication of the information, as Portal had no intent to publicize the data. The District Court ordered Travelers to pay Portal as a distinction between intent and no-intent by portal was irrelevant. The Fourth Circuit Court agreed. Other courts have ruled in reverse of this decision. They ruled exposure was not a publication that triggers insurance coverage and ended up not having to pay.

Since coverage under general liability insurance is uncertain, companies seek coverage under supplemental cybersecurity insurance policies. There's coverage for a wide range of cyber-related events. One company is Cybersecurity by Chubb, and it's mentioned in the textbook. It's a flexible insurance solution designed by a Cybersecurity expert. It covers a broad spectrum of risk disclosure of private information, copyright trademark infringement, reputational injury, systems security failures, harming third parties, and injuries as a result of system outages.

Cybersecurity by Chubb also included direct costs such as data breach notifications, crisis management of the data breach, forensic consultants, online vandalism, and things that might have been related to a data breach. In PF Changs breach, in 2016, over 60,000 credit card numbers were stolen. They paid $134,000 a year in premiums. Chubb covered $1.7 million dollars in cost for PF Changs for the forensic investigation and defense of consumer lawsuits. They refused to pay $1.9M dollars assessed by the credit card company as fines, card reimbursement, and replacement costs due to the company's failure to comply with PCI DSS.

The District Court ruled that credit card fees are not included as the "private injuries" that insurance was designed to cover. The court noted that the restaurant was a sophisticated party, and if it wanted these fees to be covered it should have bargained for them. You must carefully determine what is covered under provisions of your policies. Bargain for all the costs of a cyber event to have it included under your coverage. Think about what those costs might be. Certainly fines, fees, and replacement costs from card companies will be part of those fees, and they can be very large! An alternative to an insurance policy is self-insurance. It requires a large

-reserve of cash to be set aside. In the case of PF Changs, they would have had to set $3M dollars aside. While for many companies, that may not be a large amount of money, it still is money that you can't touch, as it's in reserve. On the other hand, if you think about a $134,000 dollars per year for premiums, you would pay that premium for 22 years before it covers $3M dollars of the breach cost, and with only paying the premium you can reinvest a lot of that other money, or use it for operation of the company. Even if you want to have the additional fines and fees covered under the policy, and you have raised the policy to $150,000 dollars per year, that's still twenty years of paying premiums before you would reach the $3M dollar cost of the breach. You need to think about that process. Do you pay a reserve to self-insure? The problem with self-insurance is that you really don't know how much a breach is going to cost you.

Protecting your work product is a very important aspect of handling a breach, particularly in breach litigation. We talked about the discovery process and how opposing attorneys and clients can come to your attorneys and ask for very specific things. That includes all communications that are relevant to the case. When you think about it, we normally communicate with each other within the company through messaging and email, and that's all recorded. It's all subject to discovery. When litigation begins, the legal department will issue what's called a litigation holder. This establishes an unequivocal preservation order. That means you cannot delete or erase anything relevant to the case. If you do, and somebody finds out, that can result in some very serious fines, and it could end up even worse than that. The litigation hold will ask for very specific material such as emails, instant messages, notebooks, printed material, drawings, or anything that the attorneys can imagine will be relevant to the case. They may define how we're now to store material that's identified by personnel in the company. In addition, we may hire professionals to assist in various aspects of investigation such as attorneys, digital forensics experts, security consultants, etc.

All material concerning the case is discoverable. However, there are ways to protect some of that. Attorney-Client Privilege is a very important one. This protects from discovery communications between the attorneys and their clients in the course of seeking and providing legal advice, and that could be the legal department and the employees of a company. While seeking and providing legal advice, it's nearly absolute. As we're discussing how to proceed with a case, or what to look for, the attorney might say to go look out in the logs and see if you can find anything that you can report to us that might be relevant to the breach. The attorney-client privilege protects communications, but not the underlying evidence. In that case what I gave you, my communication or my report back to the attorneys might be attorney-client privilege, but the logs that I'm using to gather that information is still discoverable. It covers legal advice, but not legal business advice, and the third-party communications may or may not be covered. The best advice I can give you on attorney-client privilege, is to talk it over with your legal team on how they would like to proceed in the security and litigation hold, if it occurs. Normally, they'll issue that email to everybody involved. Are they going to want you to gather the data and put it someplace or establish an electronic repository? How do they want to proceed if they do have a litigation hold?

Work Product Doctrine is more likely to cover the cybersecurity work performed under direction of the attorneys. Again, while not absolute, it is a very important aspect of the litigation process for you. Federal Rule of Civil Procedure 26(b)(3) says that a party may not discover documents and tangible things prepared in anticipation of litigation or trial or for another party. If I build a report that shows how a breach may have occurred, I can send that to my attorneys in the legal department and it probably should not be considered discoverable. This no absolute, it allows discovery if the opposing attorney may argue it has a substantial need for the materials, or the court may find a good cause to allow discovery of the work product. The consultant's work product may be covered as a work product in this, if it's prepared in anticipation of litigation.

Non-testifying expert privilege, Federal Rule of Civil Procedure 26(b)(40(D) is a very narrow privilege. It basically says that opposing attorneys cannot discover facts known, or opinions held by an expert, who's retained or employed to prepare material in anticipation of litigation and is not expected to be a witness at trial. There are some exceptional circumstances that the opposing attorneys may present that could actually make that information discoverable.

In the Genesco v. Visa case, Genesco is a retail chain that was hacked. They retained their general counsel Stroz Friedberg in anticipation of potential litigation or regulatory proceedings. Stroz Friedberg does forensics and security consulting and a number of other things to assist in breaches or in understanding digital forensic information. Visa investigated Genesco and issued $13M dollars in fines and reimbursement settlements against the banks that backed Genesco. This is a very common practice. Visa or MasterCard will issue the fines to the banks that back the company that's currently collecting credit cards. As in this case, Genesco had an indemnification agreement with the banks, which is very common. Basically, the banks said they had a fine from Visa, therefore you need to pay us $13M dollars. Genesco then sued Visa. Visa subpoenaed (require a document or other evidence to be submitted to a court of law) Stroz for deposition testimony. In other words, they wanted to get recordings and written testimony of individuals that worked at Stroz, who had worked on the case, and work product of the investigation. The court largely rejected Visa's argument considering Stroz as a non-testifying expert witness, and that Visa did not establish those extraordinary circumstances that were needed to allow that exception.

Genesco also used IBM to help define some security measures that needed to be put into place. That was also considered work product as it was consulting in technical services to assist the attorney and rendering advice. That was protected by attorney-client privilege as well as the work product doctrine.

This concludes Unit 2 for this week.

Unit 3 Part 1: Compliance

Welcome, everyone, to Unit 3 Compliance.

You'll find as you progress through your security career that compliance is one of the most important aspects of your job. In my career as CISO, I spent much of my time trying to understand what the security regulations are that controlled our industry, as well as trying to determine whether or not we were compliant with those regulations. It's really important that you understand what regulations apply to your industry. Some of those regulations are very broadly defined, and some are very narrowly defined. You need to establish a compliance program and determine if you are compliant. If you aren't compliant, what do you need to do to become compliant? What happens if you fall out of compliance? In order to control the compliance process and program many companies hire a Chief Compliance Officer. That officer works with the security team and the legal team to understand the compliance obligations of the company.

What are the compliance obligations that you're required to adhere to in your industry? If you're part of the critical infrastructure, these may very well be defined for you. The critical infrastructure are those industries, utilities, and agencies that are highly critical to the national infrastructure and the national security. What kind of industries are these? We'll look at several in the unit: the financial industry, payments industry, electrical utilities, and healthcare. Each of these industries provides critical services to the nation and we'll examine those.

There's a process called Information Sharing, and what you'll find as you go through your compliance and security program builds, is that you'll be able to share information with people in your industry, if you become part of the Information Sharing Program. This may be through an Information Sharing and Analysis Center (ISAC), or through an informal group. An Information Sharing Program was a concept that was issued in Presidential Decision Directive 63 (PPD-63) under President Clinton, in 1998. I put the context of PDD-63 in the supplemental reading, so you'll have an opportunity to read through the program. It's been refined over the years. The PDD-63 defined the concept of information sharing and analysis centers or ISAC's. This was an opportunity for public and private industries and agencies to be able to share security events, incidents, and data. The goal was fast reaction to serious security events. It defined the critical infrastructure and what those industries were that comprised the critical infrastructure. It defined the roles of government agencies and working with private industry. There was a saying attributed to Benjamin Franklin, and, quite frankly, historians don't know if this ever happened. Supposedly, he said at the signing of the Declaration of Independence, "We must all hang together or most assuredly we will all hang separately". Whether he said it or not isn't as important as the fact that coming together to share security information is an important aspect of being able to gather information about security events and security practices that can help you in your compliance programs, as well as your security programs.

Compliance regulations were developed by statute agencies, administrative bodies, state law, and special interest groups. They evolve over time to meet evolving threats. For instance, the Payment Card Industry Data Security Standard (PCI DSS) was developed through the PCI Security Council, which is a combination of credit card company representatives and industry representatives who come together to determine any new threats facing the payments industry. They modify the standard periodically.

As I said earlier, we can have broadly defined compliance regulations or narrowly defined rules. The broadly defined rules generally provide little specificity. An example we'll see is the Nuclear Regulatory Commission Cybersecurity Regulations. Narrowly defined rules provide more details of the cybersecurity programs. Some regulations provide latitude for how the Chief Information Security Officer (CISO) or the Chief Compliance Officer (CCO) meets provisions of the compliance regulations. For example, the Gramm-Leach-Bliley Act (GLBA) has certain goals and certain activities it expects to be accomplished, but it allows the CISO or the CCO to have the latitude to determine how those are implemented. The same thing applies to the Health Insurance Portability and Accountability Act (HIPAA). It expects reasonable and appropriate implementations. Almost uniformly, all compliance regulations have two common provisions: you must establish an Information Security Program, and in most cases, this must be written; and, you must have an individual who develops and directs the program.

How do we construct a compliance program? You choose a framework first. Just like the security frameworks that you would use to guide the security of your company. You choose a framework, this could be a regulation that you're subject to, or an industry standard that you're subject to, or both. Determine commonalities across security and compliance programs. Identify similar security controls that are across both programs. For instance, if I need to have firewalls and firewall rule sets in both my compliance obligations and my security framework, that's a common goal and a common element of the programs. You identify those program elements that are different, as well. Then, build a matrix of common authority. In that matrix of common authority, if you can envision this, simply write across the top the different compliance obligations you have, and write down the side, the various elements that need to be accomplished. Examples are that a firewall rule has to be implemented, or security awareness training must be provided for your employees. Then, you can check which of the various compliance rules and regulations would have that particular program element. You can use that to develop your gap analysis, when you're trying to find those things which have to be accomplished in both security and compliance. You can see that element in your matrix of common authority. When you have elements that are unique to a particular regulation, those will stand-out as well.

How do we construct a compliance program? We establish controls to ensure the program components remain in effect. Controls should be designed to clearly identify the program components. They should be observable and measurable. That does not mean measured in terms of seconds, or number of logs, or weight, but measurable in the sense that you can see it and determine is it operational, or is it not? You have defined timeframes; defined personnel responsible for each control; defined

documentation, procedures, and mitigation runbooks. If something does happen you know how to mitigate the issues. You have periodic testing of your controls. The most important aspect of the compliance program is staying in compliance! You have to update controls for updates in security and compliance frameworks, and it's critical to run vulnerability and penetration testing on a regular periodic basis. Document everything!

The one key and most important lesson I can teach you….
Compliance is NOT security!
Many companies were compromised that only met the compliance obligations, and did not look at security from a holistic point of view.

Unit 3 Part 2: Financial Institutions

Let's get into the meat of the Compliance Chapter: let's look at Financial Institutions. When we look at financial institutions, one of the major regulations comes through the Gramm-Leach-Bliley Act (GLBA). It imposes administrative, as well as technical and physical safeguards to protect data. It was designed to accomplish three goals: to ensure security and confidentiality of consumer records and information; to protect against anticipated threats or hazards to security or integrity of such records; and to protect against unauthorized access to or use of such records. It only applies to non-public personal information. If there is information that concerns you that's already out on the web or it's public information, well that's not covered under GLBA. Personal identifiable financial information is what is provided by the consumer to a financial institution, such as your name and your bank account when you're applying for a loan or resulting from a transaction with or a service performed for a consumer, or otherwise obtained by the financial institution.

There's more than one agency that regulates the financial industry. There's the Office of Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision. They all manage and regulate different aspects of the financial industry. They develop what's called Interagency Guidelines to implement a comprehensive written information security program. That should involve the Board of Directors, as well as the team writing the security program. It is designed to assess the risk and manage and control the risks that you might identify.

Let’s look at it in more depth, Manage and Control Risk. There's a number of elements that you'll recognize here, particularly if you've designed any security programs: implementation of access controls, restrictions on the physical locations of stored customer data, encryption of information in transit and at rest, and segregation of duties. Segregation of duties is a very important aspect of both security, as well as, compliant regulations. Another element is background checks on employees, and that may vary depending upon the type of financial industry you're in. More elements of Managing and Controlling Risk are: System monitoring, the training of employees on the information security program, maintaining regular testing of controls and systems, properly disposing of customer information, providing adequate oversight of service providers’ information security measures, and adjusting information as new threats arise.

Second, to establish and maintain an incident response program, you will need to determine what incident response processes and procedures you have around sensitive data. Sensitive data in most cases is defined as first name or first initial and last name, plus social security number, driver's license number, account numbers, credit or debit card numbers, personal identification numbers, or passwords that permit access to customer accounts. We saw this in Unit 2, when

we looked at a lot of the privacy rules and security rules that states defined around data breach laws. You will want to train incident responders and test the processes multiple times during the year. You can do that through tabletop exercises, or today, you see a lot of security people using virtual environments to train incident responders.

You'll want to establish and maintain an incident response program. At a minimum it should include: assess the nature and scope of an incident, set up an identification of what customer information may have been accessed, and take steps to contain and control the incident from any further access. An element that is not in the text, but which I find very important to do if you have an incident, is to contact your legal department. They will want to know as soon as possible if something has happened. As we saw in Unit 2, there are a number of processes and procedures you may have to execute if there is an incident: notify the primary federal regulator and notify appropriate law enforcement agencies; keep the customers informed as soon as practicable; notify the Board and keep them informed of the state of security. You should do this at least annually, but I always did it quarterly to keep them in the loop and allow them to provide oversight to what we were doing in security. Is this a broadly defined compliance obligation? Well, it's got a lot of specificity as to what you have to accomplish, but you have a bit of latitude on how to do that.

The Securities Exchange Commission (SEC) sets the GLBA as a requirement for brokers, dealers, investment companies, and investment advisors registered with the SEC. It's not as detailed as the Interagency Guidelines. They provide that you must have a written information security program. The procedures to ensure the administrative technical and physical obligations to the GLBA are there, but you have more latitude as to how you want to accomplish that. On the other hand, they're also very aggressive in enforcement of the provisions that they identify.

Unit 3 Part 3: Financial Institutions

Another player in the regulation of the Financial Institutions is the Federal Trade Commission (FTC). The FTC developed Safeguards Rule to regulate those institutions that are not regulated by other banking agencies or the SEC. This could include mortgage brokers and retailers offering credit to customers, or customer reporting agencies as well. The FTC did not pass detailed safeguard rules, so there's some latitude in how a program will be implemented and maintained. However, the FTC has been quite aggressive in its enforcement actions. The Safeguards Rule requires companies to develop, implement, and maintain a comprehensive written information security program; to designate an employee to coordinate the program; to identify reasonable and foreseeable internal and external risks; to implement safeguards and conduct regular assessments; to contractually require third-parties to comply with the Safeguards Rule; and to regularly evaluate and adjust information security policies and procedures.

We'll look at several cases that have involved the FTC,

In the Matter of ACRAnet, Inc.
ACRAnet assembled consumer reports for the three major consumer reporting agencies. Reports contained sensitive non-public personal information and were sold to mortgage brokers ,and, therefore, were subject to the FTC Safeguards Rule. In 2007 and 2008, hackers accessed nearly 700 consumer reports. This was through vulnerabilities in ACRAnet's clients' networks. After the breach, ACRAnet did not take steps to prevent similar incidents. The FTC cited them for violations of the Safeguards Rule. Specifically, ACRAnet didn't implement adequate customer information safeguards; didn't test and monitor their information security controls; didn't evaluate and adjust their information security program to increasing risks; and did not develop a comprehensive information security program that would be able to protect customer data.

In the Matter of James B Nutter & Company
James B Nutter makes and sells residential loans, and thus is covered by the FTC Safeguards Rule. It collects sensitive non-public personal information through a website and a computer network on which they collect the data, store it, and conduct their business. An unauthorized individual hacked the network and sent spam, but there was no evidence of theft of the customer data. The FTC noted that the hacker could have accessed the personal information, and so they cited James B Nutter & Company for violations of the Safeguards Rule. The company didn't develop a comprehensive written information security program that identified risks to personal information; didn't develop personal information risk controls or evaluate them; didn't adjust the information security program; didn't oversee their service providers; and didn't contractually maintain clauses that they would implement information security safeguards.

In the Matter of Superior Mortgage Corporation
Superior is a residential mortgage direct lender. They collect sensitive non-public personal information. The FTC complaint did not cite any data breach or attack. It was simply that the website only encrypted data in transit and not at rest. Unencrypted data were transmitted in clear text to the headquarters in branch offices. The FTC cited Superior Mortgage Corporation for not having conducted a security risk assessment; for not implementing adequate password policies for access to sensitive customer information; for not encrypting sensitive customer data at rest; and for not overseeing service providers and contractually obligating them to implement information safeguards.

The Fair and Accurate Credit Transaction Act of 2003, (FACTA), was enacted over growing concerns in the financial industry with identity theft. It required banking regulators in the FTC to develop regulations over financial institutions and creditors offering covered accounts and to develop reasonable policies and procedures to prevent identity theft. What's the definition of a creditor? That is someone who obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction; who furnishes information to consumer reporting agencies in connection with a credit transaction; or who advances funds to, or on behalf of a person based on an obligation of that person to repay the loan. The definition does not identify a creditor as one who advances funds on behalf of a person for expenses incidental to services performed by a creditor. This was important because that was the exception that took out doctors and lawyers and other people who performed services. Basically, either assumed the debt of the individual who was responsible for receiving those services, or in essence advanced the funding for the individual to have those services.

The Fair and Accurate Credit Transaction Act also defined covered accounts. These are accounts offered primarily for personal, family or household purposes. They are designed to permit multiple payments or transactions. Examples of this would be mortgage loans, automobile loans, margin accounts, and checking and savings accounts, etc. The company must have a written identity theft protection program, and identify the red flags or patterns, practices, and specific activities that indicate possible identity theft. There are several pages that list a lot of these red flags in the text and you should know those. For instance, if there are a lot of new transactions being opened up in someone's bank account or in establishing new credit cards, etc., it raises a red flag. That allows a bank to go back and question whether or not the activity was legitimate or not. The theft detection program should detect the red flags and appropriately respond to those flags. The company should periodically update the red flag program.

Unit 3 Part 4: Payment Card Industry

The payment card industry comprises companies that issue, use, and accept credit and debit cards. This includes retailers, both ecommerce and brick-and-mortar stores, as well as, acquirers and card processors. Of course, you're all familiar with MasterCard, Visa, American Express, and Discover. You may not be familiar with JCB, which I believe is a Japanese company. Those are the credit card companies that basically comprise the Payment Card Industry (PCI). All must be compliant with the latest provisions of Payment Card Industry Data Security Standard (PCI DSS). It was devised by the Payment Card Industry Council (PCI Council), in conjunction with industry leaders. The technical guidelines are established by tiers and by technologies. The larger the entity that's issuing cards, in other words, the more they accept in cards, the higher they have to qualify in the PCI standards. The more technology you use, such as payment terminals that are encrypted, there's a slightly different set of rules that you might have to follow. However, keep in mind that there are tiers, and there are technologies that help differentiate among the retailers, the companies that issue the cards, the acquirers, and the card processors. The company that's issuing or accepting credit cards must be tested annually by what's called a Qualified Security Assessor (QSA). These are individuals who are trained to look at the requirements of the PCI DSS and determine the quality and the factuality of the implementation that a company has claimed. Their network is assessed at least quarterly by what's called an Approved Scanning Vendor (ASV). ASV's are people who are trained to scan the networks and look for vulnerabilities that might impact the safe storage of card data.

There are six goals and twelve requirements in the PCI DSS. The First goal is to build and maintain a secure network in systems, and it has the things that you would expect to find in network security: Requirement 1: install and maintain a firewall configuration to protect cardholder data. When you think about it, that's looking at the firewall rules and the way the network is set up to be protected through a firewall; Requirement 2: do not use vendor supplied defaults for system passwords and other security parameters. This is exactly what you would expect if you were setting up your security program that you wouldn't keep the vendor supplied defaults, and as such is spelled out in the PCI DSS.

The Second goal is to protect cardholder data: so, Requirement 3: protect cardholder data. There are provisions in the PCI DSS that explain what that means, and how to establish technical controls that will protect that data. One of which is you cannot store full track data from a card. On the back of the card are magnetic strips, and on the magnetic strips are tracks. Each track stores information about the card: the card number, the name of the cardholder, expiration date, CVE, and other pieces of information that are critical. So, you can't store that data on your network. You can store encrypted portions of the data, but you cannot store the whole track; Requirement 4: encrypt transmission of cardholder data across open and public networks. It is very critical when you're looking at Requirement 4, that you keep in mind, it's across open and public networks. This is where we look at setting up TLS to accept credit cards into a company, as well as to protect the transmission. In addition, there are other

requirements that we'll see here shortly that require you to encrypt the cardholder data.

The Third goal is to Maintain a vulnerability management system, and it leads to Requirement 5: protect all systems against malware and regularly update antivirus software or programs. Even though one may argue that antivirus software only protects a portion of the malicious traffic you might see, it has the important aspect of saying that the company must have at least that. Many companies go much further and put software on the systems to protect against spam, to protect against spyware, etc.; Requirement 6: develop and maintain secure systems and applications. You want to make sure that you're testing your application security as well as all the other aspects of your program.

The Fourth goal is to Implement strong access control. This leads to Requirement 7: restrict access to cardholder data by business need-to-know. It goes without saying, if someone does not need to have access to it, either internally or externally, they should not have access; Requirement 8: identify and authenticate access to system components; and Requirement 9: restrict physical access to cardholder data. Requirement 9, is where you implement all your physical controls: having your systems protected from physical access, having access controls in place, and etc.

The Fifth goal is to Regularly monitor and test networks. This brings Requirement 10: track and monitor all access to network resources and cardholder data. This is where you'll set your controls for managing the access to network resources, logging that access, and making sure you know what's happening at all points-in-time with the system components where cardholder data may exist; Requirement 11: regularly test security systems and processes, which is simply the vulnerability testing, etc.

The Sixth and last goal is to Maintain an application security program. This leads to Requirement 12: maintain a policy that addresses information security for all personnel.

Credit card companies individually enforce these requirements on banks. If there is a breach of a company, the credit card companies don't necessarily go straight to the company. They go to the bank first and impose that enforcement on the bank. The bank in turn, enforces those on retailers and card processors. This is usually through indemnification clauses in the agreements between the banks and the card processors, or the retailers. Credit card companies typically use penalties, fines, fees, and replacement card costs in their estimation of the costs to enforce on a breach. Banks may also use those indemnification clauses in their contracts to take penalties against a company, or a card processor, if in fact, they are set back with some cost that they need to cover also under the breach.

Two states impose PCI DSS obligations. Nevada just basically says any merchants that are operating in our state have to comply with the PCI DSS. Washington State, on the other hand, says that you have to have reasonable care to guard against unauthorized access to payment card information. If you encrypt your data and are certified PCI compliant with the DSS, you will have a better chance

becoming exempt from Washington State imposing penalties upon you for being breached. Home Depot tried to use these defenses, but was denied by the court. Financial institutions alleged that Home Depot was not compliant with the PCI DSS. There's an interesting point there. I don't know the granular details of the Home Depot case, but I know that companies who are breached aren't necessarily out of compliance with PCI DSS. However, the philosophical view on that is if you are breached, you must not have been compliant somewhere in those requirements. It's an interesting problem that a company faces. You can spend a lot of time and effort, extend a lot of reasonable care to protect your networks, but if you're breached, you'll probably be deemed not to have been compliant with the PCI DSS at the time. The PCI DSS is the “de facto” standard of care for accepting, using, processing, or storing credit and debit card information. As far as I know, for the immediate future, it will be the standard that the payment card industry will maintain.

Unit 3 Part 5: Health Care Industry

The healthcare industry is governed by the Health Insurance Portability and Accountability Act (HIPAA). This is run by the Department of Health and Human Services (HHS). The HIPAA Security Rule applies to the two types of entities, covered entities or business associates. Covered entities include such things as health plans, health care organizations, or health care providers. They transmit health information in electronic form. Business associates are providers of data transmission services to covered entities, or a person who offers a personal health record to individuals on behalf of a covered entity, or subcontractor that creates, receives, maintains, or transmits protected information on behalf of a business associate.

HIPAA only applies to protected health information. It's collected from an individual and created or received by a covered entity. It can relate to past, present, or future physical and mental health, provision of health care, or payment for the provision of health care. It's only protected healthcare information if it directly identifies an individual or, on a reasonable basis, could identify an individual. Covered entities and business associates must ensure the confidentiality, integrity, and availability of electronically protected healthcare information. This is the same confidentiality, integrity, and availability that we've had in the security industry, for as long as I've been in the industry. You must take steps to reasonably prevent anticipated threats. Always use any reasonable and appropriate measures to implement the standards of HIPAA. HIPAA provides latitude to determine how you will implement those standards, but it does provide a fairly detailed list of the types of things that should be in place. There are four types of these called Safeguards: administrative, physical, technical, and organizational safeguards.

There are many examples of these listed in the book. I've highlighted a few here to give you an idea of some things that are contained within each of these Safeguards. Listed under Administrative Safeguards are: to manage security processes to prevent, detect, contain, and correct security violations. This is the corollary to the statement that you see in other regulations to have written security policies and procedures; to conduct an accurate and thorough assessment of potential risks and vulnerabilities; to implement security procedures to reduce those risks; to sanction non-compliant employees, and for that provision you will need to work with your HR department so that they understand the rules as to why you're protecting HIPAA data, and why there needs to be a sanctioning if an individual who has access to that data does not maintain a secure environment; to regularly review system activity; to designate an information security officer, and again that corollary that we see in other regulations; to develop authorization processes to reduce the likelihood that somebody who isn't authorized would have access to the health data; and to develop procedures to remove access for terminated employees, or for those who are no longer in a position to have a need-to-know that data.

For Physical Safeguards, think of these as how to physically protect the data. First, think about limiting the physical access to the facilities and systems that store protected health information. When I worked for a telecom company, we had to physically build walls inside the company to isolate those people who had access to health data from those who did not. Next, establish best business continuity plans; develop procedures and policies to physically safeguard systems that store the electronic protected health information. One of the things we did to protect the data was to build cages inside of the data center that went from floor to ceiling, as in cement floor to cement ceiling, so that nobody could access the systems where that data was stored. Then document all repairs and modifications the doors, locks, and other physical components; develop physical safeguards to restrict access to the individuals who are cleared to access health information. We put up card readers so that people who had their ID cards, who were cleared to enter the area where we stored health data, could enter that area. Then, develop policies and procedures for the removal of systems that stored electronic protected health information. You want to ensure if you are removing a device that had stored data on a hard disk, that hard disk is either wiped or destroyed. Likewise, with paper records, that it's either shredded, dissolved, burned, or something that will prevent anybody from having access to that data.

Technical Safeguards are what you would think about in more detail for implementing practices to protect the health data. You might want to develop technical policies and procedures to grant access to cleared individuals. You will need to have a known user ID and have emergency access procedures. We used to call this “break the glass”. If there was an emergency during off-hours, someone in the data center could give access to an administrator to take care of an issue. You need automatic log offs and specified time of inactivity. If you walk away from your screen, the screen then locks and at some point-in-time will actually log you out. You need an encryption and decryption of electronic health data, using encryption algorithms defined by NIST. You need to log activity on all systems that store electronic protected health information and save those logs. If you need to reference them in the case of a breach, you will want to make sure that you have the logs available. You need to develop procedures for verifying an individual's identity before providing access. That could be very interesting if you have individuals that are working remotely. You have to trust somebody at that site who can verify the identity of the individual. Implement technical safeguards for your networks.

Organizational Standards are usually contractual obligations. Contracts with business associates must explicitly require the business associate to comply with HIPAA security requirements. Likewise, if they use subcontractors, the subcontractors must be compliant with security requirements. Group health plans must state in their document that Plan Administrators will reasonably and appropriately safeguard electronic protected health information.

Interestingly, a breach notification is not necessary if the health information has been secured pursuant to HHS (department of health & human services) guidance and there’s a low probability of compromise. Encryption should be

an algorithm validated by the National Institute of Standards and Technology (NIST).

Breach notification may be delayed if there's a law enforcement action. Otherwise, the notification must be made within 60 calendar days. Within that notification you must describe the breach, including the date of the breach, and date of the discovery. Which means, at that point, you've already done some forensic investigation and that you know approximately the date of the breach. The notification should include: a description of the types of unsecured protected health information involved; the steps individuals should take to protect themselves from harm of identity theft; a brief description of the covered entities investigation and mitigation activities; and contact information for more questions such as a toll-free telephone number, an email address, website or mailing address.

For the notification process you can send email to the last known email address or postal address, if you have that information. Alternative notifications, if you have less than 10 individuals compromised, could be by telephone or other means. If it's over 10 people, you could do a conspicuous posting on your website for at least 90 days, or a conspicuous notice in a major newspaper. You want to include a toll-free number which is active for at least 90 days. A telephone can be used if urgent notification is needed. If there are more than 500 individuals in a single state that have been compromised, the appropriate state authorities must be notified within 60 days. You also must notify the HHS. If you'd like, go out to the website of the HHS and look at the Office of Civil Rights for cases of past breaches. They're usually fairly short and very interesting to read.

Unit 3 Part 6: Electric Utilities:

The last two topics I'd like to look at are the electric utilities and the nuclear facilities. Electric utilities are critical to our national infrastructure. Imagine the issues if the National Grid, or part of it, went down. We can see what happens by looking back at August 4, 2003. I provided an external link on the website where you can look in retrospect to what happened in 2003. With the power being out for 29 hours in the Northeast, we ended up with 11 dead, and a $6.4 billion impact on the U.S. economy. What if we have a long-lasting outage and what would that impact be? The Federal Energy Regulatory Commission (FERC) regulates the national electric utilities. There is an increasing focus on cybersecurity as the threats from external sources have been focused on the electric industry. In 2016, the FERC adopted seven critical infrastructure protection reliability standards which originated with the North American Electric Reliability Corporation. We'll look at those in in brief.

CIP-003-6 Cybersecurity- Security Management Controls. At least every 15 months, the utilities' senior managers should approve the cybersecurity policies addressing: employee training, electronic security parameters including remote access, cyber security physical security, system security management, incident response planning, incident recovery plans, configuration change management, information protection, and a response to exceptional circumstances. The senior managers are addressing those policies around the security and compliance of the utility in those particular areas where we would normally look to secure not only the facilities, but the systems, and the data. The utilities should have a security manager to guide the program. So, you have senior managers who are guiding the program, which is basically the corollary that we saw in other regulations, where there was an individual who would be in charge of the program. Since we're looking at these policies, we can assume they should be written and well documented.

CIP-004-6 Personnel and Training. There should be quarterly training for security awareness, a review of employees' criminal backgrounds at least every seven years, other background checks for individuals who access cyber security systems, the set up of a need-to-know access control program, and the timely removal of access if someone's terminated or no longer needs to have access to the facilities.

CIP-006-6 Physical Security of Cyber Systems. There should be a comprehensive plan for physical security of physical security facilities, which includes alarms and access logs. There should be an escort program for visitors, and again, all should be documented.

CIP-007-6 System Security Management. Enable only the logical network at accessible ports. In other words, there's a lot of ports open by default on most systems when you put them online. You should only allow those ports that need to be active, be active, and the rest should be shut off. Establish a patching program

so that at least every 35 days you're evaluating new security patches. Take other steps to reduce harm, perhaps vulnerability testing. Maintain audit logs and particularly look at failed log-in attempts and any activity from malicious code. Look for potential security events, which should then tell you that you'll have a Security Incident and Event Manager installed, or what we call SIEM, so that you can stay alert on the security events, as well as look for potential events. There should be procedures around login credentials. You should have an inventory of the user accounts, change default passwords, and all passwords should have a minimum length.

CIP-009-6 Recovery Plans for Cyber Systems. The utilities should have a framework to create plans for responding to cyber incidents. Identify specific job responsibilities for the incident responders. Describe how data will be stored, particularly around any encryption that you might use, and how you might segregate your networks to protect against access. Describe backup and recovery processes, and at least every 15 months, test the recovery processes and procedures. This can be a tabletop exercise, a paper drill, or a physical switch over the systems. We used this when we had a hot data center environment. We had a backup and the original systems right there. The systems were set-up so that if we lost access to one, it would immediately go to the other. Every once in a while, we would test it by actually pulling the power switch on one set of systems, and let it switch over to the other set of systems. Every 36 months conduct an operational exercise of the recovery process.

CIP-010-2 Configuration Change Management and Vulnerability Assessments. These are critical! Develop a configuration change management process and follow it. Usually you set up what's called a Change Control Board, so that as changes are anticipated, they're presented to the Change Control Board. Those individuals can understand whether there's going to be impacts on their parts of the operation, as well as, what you're changing. First you want to establish a baseline. You need to understand what operating systems you have, what software you have, what ports you're using, and make sure that everything is patched. Then you can document any changes from the baseline, at least every 35 days. At least once every 15 months you want to conduct what's called a Vulnerability Assessment, and this is where you’re looking in all your systems, all of your networks, and looking for vulnerabilities that haven't been discovered, or may affect your operation. Personally, I always have the systems folks do those vulnerability assessments every 30 days, particularly against very critical systems, and less often for those systems which are less critical. I would never wait 15 months to do that! After 36 months assess the vulnerabilities against your baseline, and then reset your baseline. You should have to authorize the use of removable media. If you allow removable media, you need to set up policy and procedures of how it is to be used. Examples are thumb drives, portable disk drives, or whatever media you want authorized prior to their use on your network. Set up policies and procedures around their use.

CIP-011-2 Information Protection. You must provide Data protection, regardless of whether the data is at rest or in transit and prevent unauthorized removal of data from your network.

Nuclear Regulatory Commission (NRC). U.S. authorities are deeply concerned about cyber threats to our nuclear facilities. The NRC adopted cybersecurity regulations for licensees and nuclear power reactors back in 2009. However, the concern over cybersecurity capabilities of Foreign Assets necessitated the creation of the Cybersecurity Directorate in 2013. This oversees the cybersecurity of the nuclear industry. NRC regulations protect nuclear facilities from cyberattacks, reduce likelihood of those cyber incidents, and mitigate harm caused by cyber incidents. There is a great deal of flexibility on how to draft and implement these plans. A written cybersecurity plan must be developed, again the corollary back to what we see in other regulations, but, comparing it to other regulatory frameworks, it's actually a much less detailed framework. It does allow the security manager to implement those controls which are necessary to protect the systems. Personally, I want to ensure nuclear facilities are very well protected.

This is the end of Unit 3

Unit 4 Part 1: Security and Compliance Adviser

Welcome to Unit 4. The topic I'd like to discuss in Unit 4 is another task that the security leader is counted upon to undertake from time to time, and that is as a security and compliance adviser. Periodically, you may be asked to comment on the state of security and compliance. The question is: from whom might these requests come? What do you really advise? For that matter, what is the "state" of security? What topics of security and compliance would you cover? What degree of detail does the security leader provide?

The security leader may report on the state of security compliance on a periodic basis. That may be very regular, such as quarterly or annually, or it may be really periodic. From time to time, somebody will come to you and ask you to describe the state of the security operations that you have. To understand what we're talking about, you have to establish two concepts. First, what does it mean when we say: "state of security and compliance"? How often is "periodic"? According to Merriam-Webster, the state of something is a mode of condition or being, such as a state of readiness, or a condition of the mind or temperament, such as a state of nervousness, or a stage in the physical being of something. I like to think of "state", from a security perspective, as incorporating all three of these definitions.

First, let's look at mode of condition or being, such as the state of readiness. This is the easiest to understand with respect to security. We talked about setting up a security or compliance model in earlier parts of the course. So, you'd want to look at things like the gap analysis. What is it that you're missing in your security framework or your compliance framework? Then, of course, you need to address your gap mitigation. How am I going to fix the things which are identified as gaps in my analysis? Then you need to maintain a continual review of that readiness of security or the compliance program itself. We provide these type of readiness reports from a number of different publications, requests, etc. For instance, for 10-K's and 8-K's, there will be security comments. The Board of Directors often asks for the state of security. As part of their job as fiduciaries of the company, they must understand whether or not the company's security and compliance obligations are being met. The Board will come to you at least annually, and I would suggest meeting with the Board of Directors quarterly, at the least, to be able to provide that condition and/or state of security. Insurance brokers, such as your general liability insurance brokers or the E&O brokers, will certainly want to meet with you to understand the state of your security so they can price your insurance policies. For Auditors and Assessors, there's an annual audit by the IT security auditors, and certainly they'll want to know what elements of security are in place, where there might be gaps, and whether you have obligations under a certain regulation or standards, such as the PCI DSS. Those Assessors will come in at least annually to be able to provide their statement on the state of your security. Of course, clients sometimes will ask for your state of security. That may often be in the form of a questionnaire, or you may agree to have a client come in and do an on-site audit. In some of the contracts we produced, we would have clients who would request the right to audit, and we would grant that in many cases.

If we look at security as a condition of the mind or temperament, we might be asked to provide an assessment on the temperament of the security community. For instance, think about an event that might take place, for example “WannaCry”. Certainly, somebody on the Board, or senior management, or a manager, or another employee may ask, “How is security approaching this particular problem?”. So, we look at not only the physical things that we do, but the question of whether or not the event we're looking at, implicitly or explicitly, requires that we turn our attention 100% to that event. There may be, for instance, a malicious attack out in the wild that may not be a very high-risk to us, so this certainly would not be something that we would want to drop everything and go and try to fix that particular problem. Generally, we’re looking for the state of an external condition situation or event though it's not unbelievable that some internal event also could generate a question of our assessment of the security of that particular event. For instance, somebody may be creating a new type of product, and they would like our input on the security of that product and anything more they would need to do to make it secure. An example of this is: how aggressive are malicious actors pushing ransomware attacks this month? We may look at it one month and see that ransomware is really hitting hard on the landscape of security, and so may do a special security awareness session that month. The next month, it may not be as high of a risk and we may not do anything special on it.

If we look at security as a Stage then, think of physical being of something as something like project management. We're undergoing a number of security and compliance projects at any point in time in the operation of a security or compliance group. Each of those projects has a state of completion, or a stage in which it is operating. We think of these as 50% done or 75% done, etc. It may also be how the completed products, or completed stages, really influence the security that we'll have after the project is done. For instance, we may say we already have the most important elements of security implemented in this project, and, therefore, what we have left to work on is the user interface, or something less impactful on security, but certainly a part of the project. An example is a network segmentation project. As you segment your network, the more segmentation you do, the stronger you may be building your security model. However, not every segmentation necessarily changes the security around sensitive data. Therefore, you can measure how much of the project is complete and how much the “completeness” impacts your goal of protecting sensitive data.

So, who might be asking us for these comments? Certainly for 10-K’s or 8-K’s, which we'll talk about in the next section, this might be senior management or the Board of Directors asking you directly to provide written comments on the state of our security. The Board of Directors is actually just the board asking you to provide them a current state of security so they'll have a feel for how the security of the company is being managed. As I said, the insurance brokers could be cyber insurance brokers, E&O brokers, general liability brokers, etc. The appearance of assessors and the auditors will be almost guaranteed to happen in any security operation. As I said, you'll have your annual IT security auditors, and there you'll provide a very detailed assessment of where the security model sits at that point in time. They'll ask you very specific questions, either in a questionnaire form, or in person, and they will document it very

heavily. The same thing with compliance assessors, although their audits may not be quite as heavy as an IT security auditor, it's important to document the elements of security that are identified through those assessments, particularly, any gaps which need to be mitigated rapidly. Project status questions come from senior managers and Board Members, and also from other team members who are coordinating their projects with yours. To improve the overall state of security, everyone in a company may be part of that process through the security awareness training, questions and answers, town halls, etc. Senior Management, the Board, and the clients will all be interested in understanding what the state of security is at any point in time.

What do you advise about?
That depends upon the audience and the tolerance for detail. We looked at the audiences to which you might be providing detail, and each audience might have a different view of what's important to it. More importantly, some audiences may also have a different view on how much detail they'd like to get. For instance, Boards tend to like very concise elements of security provided to them in 15, 20, 30-minute intervals, informing them what is the state of security. They have the option, at any point in time, of asking questions and asking for more detail, but they want succinct presentations on the state of security. What I used to do would be to provide very succinct details of security, but, then also, provide written detail in much greater depth, which the Board of Directors could read through at its leisure. If the Board members had questions, they could read through it in more detail and ask those questions, or simply read parts of the report that were important to them. The level of detail to provide comes with experience. When I first started presenting my details to the Board, I really felt for the Board Members because the presentation was excruciatingly detailed. I finally sat down with the General Counsel who said it's all great detail, but far too long. That's when we devised the plan that I would do a much shorter presentation and provide written details to the Board of Directors.

Unit 4 Part 2: Security and Compliance Adviser

Periodically, you may be asked to summarize the state of security or compliance for an 8-K or a 10-K, which are defined by SEC Regulation S-K. The 10-K is a required SEC annual filing for publicly held corporations. You can think of a 10-K as somewhat of an annual report on steroids. You may be very familiar with what an annual report is and the types of information that you find there. The 10-K is a much more detailed description of the financial condition of the company. There are certain types of information which generally are included in the report. I've listed these on the slide, such as the history of the company, organizational structure, financial statements, earnings per share, the subsidiaries of the company, the executive compensation, and other relevant data.

There are many required sections of the 10-K. One is Business, which is a description of the company and those products and services that the company provides. Another section is Risk Factors where you list in order of importance the risk factors facing the company in the past, present, or future. Depending upon how much detail was provided in the 10-K about these risks, you may report on compromises in the company that occurred several years back, which may still have some lingering impact on the company. You put out selected financial data, so this may be financial information for the past five years, but you're focusing on recent performance. This is selected financial data and not the detailed financial statements of the company. Another section of the 10-K is Management's Discussion and Analysis (MD&A), which allows the management team to provide an analysis of the financial condition of the company. It's an explanation for those things that you may see in the financial reports or in the financial data that explains either good or bad performance over the previous year.

Another required section is the Financial Statements and Supplementary Data. This is where you'll have those audited financial statements, the income statement, the balance statement, and the statement of cash flow. Also, you will have a letter from your independent auditor stating the scope of the audit that they performed.

Security and compliance risks generally appear in three sections of the 10-K: Risk Factors, which is fairly obvious, Management Discussion and Analysis, and in the Financial Statements and Supplementary Data.

In the Risk Factor section, the most significant factors that make the offering speculative or risky are defined. If you think about cybersecurity risks, they may increase or may certainly impact the risks that face the company. For instance, if you have credit card data that you collect, process, and transmit, then those risks certainly are higher than a company who does not process or store credit card data. You certainly want to analyze what the risks are, either from such a cybersecurity perspective or a general security or compliance perspective, that could impact the company. It doesn't mean that there is a problem with your operation, you're simply describing those parts of your operation which could add to the risk factors of the

company. What you're trying to provide is information for the investing public on which parts of the investment are speculative or risky to their investment. As I said, this can either be detailed, or less detailed, but it has to be a complete description of the risks. This reminds me of a time that I had students do case studies. The first thing they would ask is: how many pages do I have to write? It's irrelevant! You want to provide a complete description of the risks. If that can be done in a paragraph, great! If it takes three pages, great! The object is to provide a clear picture of the risk, not to limit it to a certain amount of space in the 10-K. You want to consider all the relevant information, particularly prior cybersecurity incidents where there may have been either data lost, or not lost. You might want to talk about the severity, the frequency, the probability and magnitude of future risks. This is where you can go into more detail of how you have established a cybersecurity or compliance framework to protect against the loss of data, or intrusion, or compromise by an outside force. It's not just about consumer information; you also will need to cover intellectual property, interruption of business, or any other element that could impact the performance of the company.

In the Management Discussion and Analysis section, this is where you'll have discussions on the changes in the company's financial condition, such as the results of operations. But, the detailed financial statements, as I said earlier, are not in this section. Here you're looking at "any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income from continuing operations". What you're looking for here are unusual events or transactions, which certainly a cybersecurity event would be classified as. You're looking for materiality, meaning the materially affected amount of reported income. Materiality is certainly an interesting concept; there's no real set amount that makes an amount material in your reporting, but it is an amount that the company feels had a negative impact on the financial condition of the company. For some companies that may be a very small number, and for other companies that may be a very large number. Materiality has to be understood and explained if it relates to a cyber event in that section of the report.

In the Financial Statements and Supplementary Data section, you may have some reporting of the cybersecurity framework and compliance framework that you're using. Generally, you're describing the development of business over the previous five years. If you have a cyber incident that materially affected the company, you certainly might talk about how that has impacted the company over those five years. You may look at products, services, relationships with customers, relationships with suppliers, and the competitive condition that any of these cyber events may have impacted, due to its effect on the company. In the textbook, there's a very detailed example of how Walmart reported their cybersecurity risks and framework in their 10-K, and a less detailed example by Berkshire Hathaway. Neither of them is either right or wrong. Certainly, you have to be careful that you're not providing enough detail for somebody outside the company to use that detail to attack your company. On the other hand, you don't want to have so little detail that it doesn't adequately describe the risks associated with that cybersecurity framework.

The other document you may be asked to comment on is the 8-K, which is called the "Current Report". Certainly, if you're disclosing data breaches to investors those comments will appear in the 8-K. Therefore, you should file it as quickly as you can, and "disclose the costs and other consequences of material cyber incidents". If somebody comes knocking on your door looking for open ports, etc., you're not going to report those in an 8-K. But, if somebody comes in and steals 100,000 credit card records, you'll certainly disclose that in an 8-K. It's interesting because there's no timeframe on when you have to file this, but, if you remember back to Unit 1, we talked about disclosure to the State's Attorney Generals. If you have a breach, this has to be disclosed to the State's Attorney Generals, and that's public record. If people see disclosures to the State's Attorney Generals, but they don't see a corresponding 8-K also hit the street, then they'll start pressuring the company to produce that 8-K. The longer you wait to produce the 8-K, then the greater the impact on your reputation as a company. At the end of the day, it's not a required filing. However, most responsible companies will file an 8-K to describe data breaches to their investors, so that the investors have a clear picture of the breach, and its impact on the company.

Unit 4 Part 3: Fiduciary Duty to shareholders and Derivative Lawsuits arising from data breaches

Let's finish up Unit 4, by looking at several different additional topics. The first of which is Fiduciary Duty and Derivative Lawsuits. Fiduciary Duty is simply a duty imposed on the officers of a company to make decisions that are in the best interest of the company. We occasionally see derivative lawsuits filed against company officers by shareholders claiming that the company officers are responsible for a harm by breaching their fiduciary duty and allowing that serious harm to occur. Typically, the Board of Directors will not approve a lawsuit on their own officials. Therefore, the plaintiffs have to file a derivative lawsuit asking permission to file a lawsuit on behalf of the officers. However, under the Business Judgment Rule, the courts tend to back the officers of a company, pending evidence to the contrary, and support that these decisions were, in fact, in the best interest of the company. To pursue a derivative lawsuit, you must show that the Board exercised bad faith.

What is bad faith? Well, bad faith can be one of three things that happens: the directors intentionally acted with mal-intent; the directors intentionally violated the law; the directors intentionally failed to act in the face of known duty, disregarding their responsibilities. In the case of data breaches, it's this last scenario "failing to act in the face of known duty" that's generally the approach taken. There haven't been any successful cases of derivative lawsuits to-date, but it's something to watch.

The Committee on Foreign Investment in the United States (CFIUS) is an interesting topic to look at. Every day we see companies purchase other companies in the U.S., and some of those purchases get more scrutiny than others. However, when a foreign company wants to purchase a U.S. firm, there may be some additional scrutiny, particularly, if that company is in the critical infrastructure or if it's a defense company. As you look at the components, the people who make up the CFIUS Committee are: Attorney General, Homeland Security, Secretary of Commerce, Secretary of Defense, Secretary of Energy, U.S. Trade Representative, and Director of the White House Office of Science and Technology. This is most of the cabinet as well as some of the President's staff.

A case that the textbook brings up is: Japan's Softbank purchase of Sprint, which I believe was in 2013. There was concern that the purchase would lead Softbank to direct Sprint to purchase telecommunications equipment from Huawei and ZTE, both of which are Chinese firms. If you remember when we talked about critical infrastructure, the telecommunications sector is part of our critical infrastructure. CFIUS and the House Intelligence Committee expressed a concern that incorporating the equipment of Huawei and ZTE into the national telecommunication infrastructure could be a risk. Sprint and Softbank, however, pledged not to purchase any equipment from Huawei and ZTE. With that pledge, CFIUS basically stamped the purchase agreement and off they went. However, we're still seeing the same argument today. Particularly, as the infrastructure tries to move to 5G, and Huawei has 5G equipment which is being used in other places. It'll be interesting to see how that argument continues forward. Will CFIUS block any purchases of companies that

are wanting to purchase Huawei 5G equipment to place inside our national telecommunications infrastructure?

Another interesting case is: Export controls and Wassenaar. Export controls have long existed on the sale of certain types of equipment: military weapons, military aircraft, missiles, dual use equipment, and deemed export. Years ago, I used to have to deal with the International Trade Regulations on Arms (ITAR) because my company was using encryption technology. We were an international company, and it was not possible, at that time, for me to ship encryption technology over to one of my foreign offices. Today, there's also concern about dual use equipment that may be used in your infrastructure that could also be used in a military infrastructure. Some countries are not allowed to purchase directly any dual use equipment. Deemed exports is a very interesting aspect of the export control rules. For instance, if we write software to develop an intellectual product here in the U.S., there are certain countries that we can't allow people from those countries to help work on that software. You must look at the export control lists to determine which countries we can actively work with and which countries we can't. You can go to the U.S. Department of Commerce, I believe it is, to submit your plans to receive a letter that says it's okay to work with engineers of that particular country, and it won't be considered a deemed export.

The U.S. was a signatory to the Wassenaar agreement, which is an agreement on export-controlled laws, but it's not a formal treaty. The U.S. has passed regulations to comply with Wassenaar over the year. In 2013, the Wassenaar arrangements were amended to add intrusion software to the list of export controls. This is software that's designed to avoid their detection by monitoring tools, and protective countermeasures. The software performs the extraction of data or information from a computer or network, modifies the underlying system, or modifies an execution path to run alternative processes or malware. The software has a lot of punch to it if you're doing security research, or if you're trying to set up a subversive operation to surveil a company or a person.

Let's begin this unit talking about the Computer Fraud and Abuse Act (CFAA), which was codified in 1984 and amended in 1986. This was one of the first laws or statutes that focused on electronic crime. At the time, Congress was concerned about hacking efforts against financial and government sectors, but to appreciate these two statements, we have to think back to what the internet was in 1984. Let's start this unit off with a little history lesson. It frames the discussion on the CFAA and it shows how forward-thinking the law makers were at the time. The question I pose to you is, what was the internet before iPhones and Chromebooks?

Prior to the internet, computers were standalone, which had a very secure protocol for sharing data. I would copy the data on to a floppy disk drive and walk it over to the other computer and copy it there--fairly secure networking. However, some computers talked to each other using proprietary networking protocols, such as the systems network architecture developed by IBM in 1974. It was a complete networking protocol that could link computers together and they could talk. There was a lot of overhead though in bringing the SNA Network to life. The concept of the internet goes back even further than this. In 1962, J.C.R. Licklider, the head of the Defense Advanced Research Project Agency (DARPA) proposed the concept of the "Galactic Network". This was a very science fiction titled concept of linking computers talking to each other.

Licklider published a series of memos on the interconnection of a large number of computers at a global scale. What does that sound like? His intergalactic computer network followed on the heels of Leonard's research on packet switching. When you think about it… to connect all those computers together in that intergalactic computer, you needed to have some way for those computers to convey information to each other. Packet switching was one of the first steps in that direction. Larry Roberts and Tom Merrill linked two computers together using packet switching between Lincoln Labs in Cambridge, Massachusetts and the System Development Corporation in Santa Monica, California. These were the first two computers to talk to each other over a phone link. For those of you who go far enough back to remember the first 300 baud modems, you can imagine how slow and painful this must have been. As we always see in the

computer world, that next step forward seems like a very large leap forward. At that time, to be able to communicate over that phone link was amazing. The response times were slow with really no guarantee of reliability, but the computers were connected. They published a paper in 1966 about their efforts.

The ARPANET was funded in 1968. Bolt Beranek and Newman Company developed the interface message processors which would connect nodes to a network. UCLA and Stanford were the first two research labs that were connected in such a way. The nodes continued to be added to ARPANET. In 1969 we were up to a whopping four in total. But we needed some kind of communication protocol, sort of like a network control protocol, which was developed in 1972. After we started seeing computers connecting to the network, we started to hear the concept of the next hot application. I remember these conversations well. What would be the next hot application that would be applied to computer operations? ARPANET demonstrated the first of these in 1972. It was something called email. It allowed two computers to send and receive messages from each other. It was very simple at the time: either you sent a message or you received a message. It was very easy in those days to programmatically build your message and send it out because the software just accepted or received the message.

The development of the Transmission Control Protocol/Internet Protocol (TCP/IP) in the 1970's was accomplished by two men, Robert Kahn and Vint Cerf, often referred to as the Grandfathers of the Internet. TCP/IP was the standard networking protocol adopted by ARPANET. In 1977, a three-network connection was made between the U.S., England, and Norway. The thinking was not just connecting to computers but connecting to networks of computers. In March of 1982, the US Department of Defense declared TCP/IP the standard for all military computer networking. At this point, they were still two years out before the codification of the CFAA. Before that law came out, and around the time of March 1982, estimated statistics are that 60,000 computers were connected to the network. That number may be a low one, but it was a very small network of computers at the time.

In the 1980's, the primary use of ARPANET was research-oriented. However, the Internet service providers began offering commercial access to the computers. This is where the growth of the internet began. My company, for instance, connected to the Internet network at this point in time. It allowed us to communicate with offices in other parts of the country. It also allowed us to use email service to communicate between those various offices. Keep in mind that we're not talking about the way you think of networks connected today. There was quite an effort then to be able to hook your computers into a system that would allow you to communicate over this network of computers. In 1990, the commercialization of the network was in full swing. We had companies such as CompuServe and AOL out there servicing commercial clients.

There was one major innovation missing from this equation: one additional hot application that needed to be put into place before this intergalactic network could actually take place. Tim Berners-Lee, a researcher at the CERN in Switzerland developed what he called the hypertext language to link documents across this network. This resulted in what was called the World Wide Web (www). In fact, when you type in a link, it begins with www. Again, in the early days, this was really meant to tie one document to another. You can imagine the leap when people realized they had a method to link all of their "documents" on a site. In essence, that became a webpage, which could then connect to other webpages, which could connect to other content or documents. This provided that seamless connectivity between the documents on the site and it provided a visual context of the information that existed on your site. This was a giant leap! So, between TCP/IP, that interconnection using packet switching and hypertext language, we could now build sites that brought business-value to the network.

In 1995 the Federal Networking Council (FNC), passed a resolution defining the term "Internet". This refers to a global information system that logically links by a unique address based on the Internet Protocol and allows the computers to communicate using the TCP/IP protocol suite. This

provides users, and makes available services layered on top of that TCP/IP. When I think back over the development of the Internet, the first time that I can recall a commercial use of the internet was Toyota advertising their vehicles on the Internet. There may have been others, and somebody may very well come up with a different example. But I remember with amazement, when I saw this commercial of Toyota vehicles on the Internet, that I fully understood the internet had real business value.

The Computer Fraud and Abuse Act was codified in 1984 and amended in 1986. It was concerned about hacking and financial institutions and government agencies. Later in this unit, we'll look at a special case that was filed under the CFAA in 1988. They needed an estimate of the number of computers damaged for the case. Prosecutors estimated, at the time, 10% of the computers connected to what would become the Internet, could be subject to the CFAA. An estimate of the total connected computers at the time was approximately 60,000 computers.

The Computer Fraud and Abuse Act was a primary U.S. Federal Statute. It prohibits and criminalizes certain activities taken by an individual that "lacks authorization" or "exceeds authorized access". There are seven subsections that define various acts deemed illegal under the CFAA. Again, we'll look at those later in the unit. What do "lacks authorization" and "exceeds authorized access" mean? These terms aren't specifically defined in the CFAA, so we need to look at case law to try to determine what those terms mean. However, the defendant must play an active role of entering a computer and either obtaining information or causing damage. Passively receiving information and nothing more does not constitute access under the CFAA. In the case of Role Models America Inc. v. Jones: Jones took some information to another organization called Nova and used it there. Nova did nothing more than receive the information that the principal was not entitled to. The Court determined that "access" is an active verb, meaning to gain access to or to exercise the freedom or ability to make use of something.

What constitutes an act "without authorization" or an "excess of authorized access" ? Authorization is undefined in the statute completely, but exceeds authorized access is defined to mean accessing a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter. What kind of actions constitute exceeding access? Both of these terms lead to some of the most commonly litigated issues in the CFAA cases: whether a user has exceeded authorized access, or whether a user has accessed a computer without authorization. The courts have looked at the terms of these two

ways of looking at the issue, both narrowly and broadly. We'll look at what that means.

The narrow view of "exceeds authorized access" and "without authorization" leads to several very important cases. The first is United States v. Nosal: in 2012, David Nosal, an employee of an executive search firm, convinced is ex-co-workers to access their company's computers and provide him with confidential information. He was going to start a competing firm and he needed that information to start the firm. The government charged Nosal with aiding and abetting his ex-co-workers and exceeding their authorized access to the network with intent to defraud. This seems clear to this point. Nosal, however, successfully argued that he did not exceed authorized access and that the CFAA only covers hackers and not those who misuse information to which they had authorized access. The court agreed with him; you can see in this particular case that, although there was what appeared to be exceeded authorized access or using the information without authorization, it wasn't done by Nosal.

WEC Carolina Energy Solutions LLC v. Miller, also in 2012: the WEC argued that, before leaving the company, Miller used his access to company computers to download confidential documents about the company projects. He went to a competitor and used that downloaded information to make a presentation to a potential customer. I have to tell you that I've seen many, many, many cases of this particular type of activity. Someone's leaving a company, copies confidential information, downloads the information and takes it with them. This is a very common activity. Miller was charged with using the information "without authorization" or "in excess of his authorization". The Fourth Circuit argued that the terms are virtually the same. Importantly, the Court argued that neither term can be read to mean "improper use of information validly accessed". The Court was saying that he had valid access to the information at the time that he downloaded and copied it, so he did not have unauthorized access or exceed his access.

In the United States v. Valle: Valle, a New York PD officer, was charged with crimes arising from online communications where he discussed committing sexual violence against women that he knew. Allegedly, he used his access to law enforcement databases to obtain home addresses, birth dates, and other information about women in cases. The prosecutor argued a violation of CFAA since Valle knew that the NYPD policy was that information in the databases was strictly for law enforcement use. The Second Circuit held that Valle did not violate the CFAA. The Court held that the evil to be remedied by CFAA was trespassing into computer systems and data. Valle had authorized access to the databases that he was viewing. The Court described "authorization" and "exceeds authorized access" as ambiguous. Thus, it chose to interpret criminal statutes as "ambiguous"--in favor of criminal defendants. This is a very narrow view of the terminology and the application.

A broader view of "exceeds authorized access" and "without authorization" is also illustrated in several court cases. One important case is EF Cultural Travel BV v. Explorica, in 2001. EF Cultural brought a CFAA claim against their competitor and competitor employees. Explorica employees used an automated program to scrape pricing information from EF Cultural's publicly accessible website. So, just imagine, they wrote a program that looked at their competitor's site, scraped the information off of it, and built some type of a database. They could then see the price the competitor was charging, the types of tours, etc. These employees previously worked for EF Cultural and had a confidentiality agreement and could not disclose or use any information for a third-party's benefit or against EF Cultural. So, the Court ruled in EF Cultural's favor saying that the scrapers used tour codes to mine EF Cultural's data and those tour codes could only be known by those employees who previously had access to the EF Cultural site. There was no allegation that scraping violated explicit terms of use or workplace policies. However, the fact that the employees did have previous access was important in the court's decision that CFAA should be applied in this case.

In the United States v. Rodriguez: Rodriguez was a former Social Security Administration (SSA) customer service representative. The SSA policy prohibited employees from obtaining information without a business

purpose. Rodriguez for some reason refused to sign forms acknowledging the policy. He accessed Social Security records of 17 individuals without a business reason and was convicted of violating the CFAA. On appeal, he argued that he did not exceed authorized access because he only accessed databases that he was authorized to access. The Court rejected his argument as he had accessed data for reasons unrelated to his job. He had been explicitly told that he was not permitted to obtain information for any purpose that was not business-related.

Further, Rodriguez argued that he did not exceed authorized access because he did not use the information in a criminal manner. The Court rejected this argument as well. They stated that the manner in which he used the information was irrelevant in deciding whether he violated the CFAA. The inquiry for the court was whether he obtained the information in violation of the statute. This is considered a broader reading of the CFAA because the court was not just concerned about whether the access was not authorized, but that the access in this case was used in the furtherance of unauthorized activities.

In the United States v. John: John was a Citigroup employee and used her credentials to provide information about corporate customers' financial accounts to her half-brother. He used that information to commit fraud. After being charged under the CFAA, she argued that she only accessed what she was authorized to access. The court, however, ruled that authorized access may have use limitations on the use of the information that you see. The user knows or reasonably should have known that she was not authorized to access a computer in furtherance of or to perpetuate a crime. Further, Citigroup's internal policy expressly prohibited misusing confidential information. This was key in the court's decision. The evidence and demonstrated evidence were that John had been trained on the policy and should have known she was not able to look at this information, nor pass it on to her half-brother, in furtherance of his crimes.

Let's begin looking at the seven sections of the CFAA. You can see the seven sections here: Section (a)(1) to Section (a)(7): Hacking to commit espionage; Hacking to obtain information; Hacking a federal government computer; Hacking to commit fraud; Hacking to commit damage; Trafficking in passwords; and Threats of hacking. If you think back over to what I said earlier in the unit, when the legislators were developing the CFAA, the focus was to prevent hacking of financial institutions and government computers. That is reflected in the different sections of the CFAA. However, you'll see that certain sections are applied more broadly when they're looked at in certain types of crimes.

Hacking to Commit Espionage, Section (a)(1) prohibits an individual from: knowingly accessing a computer without authorization or exceeding authorized access; obtaining classified information; willfully communicating, delivering, transmitting, or causing the communication, delivery, or transmission to another person who is not authorized to receive that information. In other words, if I take information and give it to somebody or transmit it to somebody who's not authorized to receive that information, it is illegal. The statute also covers willful retention of data and failure to deliver it to an employer who's entitled to receive it. This only applies if the individual has reason to believe that the information could injure the United States or to the advantage of another nation.

It's rare that we see prosecution under Section (a)(1). Generally we'll see prosecutions under the Espionage Act, which we'll talk about a little later in the course. The violations for Section (a)(1) offense are felonies with up to ten years in prison and a fine, and 20 years if it's the second or succeeding violations.

Hacking to Obtain Information, Section (a)(2) prohibits individuals from: intentionally accessing computers without authorization or in excess of authorization; obtaining information contained in a financial record of a financial institution, card issuer, or a consumer reporting agency and information from any federal government department or agency, and from any “protected computer”. Protected computer, as it was originally designed, was any computer used by any financial institution or the federal government, that was used in or affecting interstate or foreign commerce.

We'll see how that term of protected computer was actually applied more broadly. It's easy to show how a computer is used in interstate or foreign commerce because you can see its use.

This Section (a)(2) is used very frequently and is one of the most commonly used sections of the CFAA. A very broad interpretation of "protected computer" is now being used and the term "obtaining information" also is very broadly applied. It includes mere observation of data and does not require actual removal of the data. Now here's an example of this particular statute. Let's say a computer service representative working in a center has the view of a screen containing confidential data such as the user's credit card data, names, addresses, etc. The rep writes down that information and sticks it into his pocket. He viewed the data; he did physically remove it from the system; he was authorized to have access to the system; but, what he did with that authorization exceeded his authorization. This brings up that vision in my mind as an example of violating Section (a)(2).

The most significant barrier to a charge or claims under (a)(2) is that the requirement of the act of obtaining is intentional as opposed to mistaken inadvertent or careless acts. If you think back to my example with the service representative, certainly viewing the data and writing it down is contra point to the policy of the company would mean it was intentional. Writing it down and putting it into his pocket certainly would not be inadvertent.

Felonies and misdemeanors could be charged in this crime. If it's a misdemeanor, there will be a fine and up to one year in jail. For a felony, there is a fine and up to five years in prison. For the felony to be applied, the offense would have been committed for commercial advantage of private financial gain; and the offense would have to be committed in furtherance of any criminal or tortious act violating the US Constitution or any federal or state laws. Once more, going back to my example with the service representative, that means sticking the information in my pocket is one thing and I've certainly violated the company policy. However, once I

commit a fraud with that information, now Section (a)(2) applies because now a crime has been committed.

Section (a)(3)—Hacking a Federal Government Computer-- prohibits individuals from intentionally accessing non-public federal government computers without authorization. These are computers that are exclusively for the use of the government and not for public computers used by the government for things like public websites. There's a little confusion here between (a)(2) and (a)(3). So, (a)(2) explicitly prohibits certain acts of federal government computers. Section (a)(3) differs and prohibits the mere act of intentionally accessing a federal government computer without authorization. Section (a)(3) is not relevant if data is obtained because that's probably covered under (a)(2).

Section (a)(2) requires both access without authorization and exceeding authorized access. Section (a)(3) requires only intentional access without authorization. Section (a)(3) applies to non-public government computers. So the website of a government computer is not covered under (a)(3) because it's publicly viewable and accessible. A first-time offense under (a)(3) is a misdemeanor. A first-time offense under (a)(2) is a felony. Thus if applicable, prosecutors will charge under (a)(2) rather than (a)(3).

Hacking to Commit Fraud Section (a)(4) prohibits individuals from knowingly, and with intent to defraud, accessing a protected computer without authorization or exceeding authorization; and furthering the intended fraud and obtaining anything of value. It does not apply if the object of the fraud was just the use of the computer and the value of the use is less than $5,000 during any one-year period. What comes to mind in this case is somebody who gains access to a computer for Bitcoin mining and simply does that. They're looking for computer time or they're looking for CPU activity. They're not looking to take any information. This is similar to mail fraud and wire fraud statutes. It's meant to capture fraud conducted over a computer.

Continuing with Section (a)(5) Hacking to commit Damage—this statute prohibits three types of behavior all related to damaging a computer. Let's look at these individually. Section A is knowingly causing the transmission of a program, information, code, or command resulting in intentionally causing damage without authorization to a protected computer. Section B is intentionally accessing a protected computer without authorization resulting in recklessly causing damage. Section C is basically the same thing with, however, a slight variation—that is intentionally accessing a protected computer without authorization and as a result of such conduct causing damage or loss. So you notice in the difference between B and C, there is in B the term "recklessly" causing damage, and in C, it's just causing damage. One or more of these are commonly prosecuted and litigated provisions, and in some cases, you may see multiples of these. They cover things like viruses and malware; denial of service attacks; and deletion of data.

Section (a)(5)(a) the first of these sections has four general elements. The first is knowingly causing the transmission of a program, information, code, or command that intentionally causes damage to a protected computer without authorization. You can see this clearly fits the pattern of viruses, trojans, etc., but the biggest hurdle is showing that a transmission occurred. One case that comes to mind is International Airport Centers LLC v. Citrin. Citrin was a former employee needing to delete proprietary data from his laptop before leaving the company. He installed a secure erasure program to irreversibly delete the data. Installing that secure erasure program constituted a transmission. He downloaded the software and he executed the code to securely delete the data. This was very much like a worm that goes through and deletes the data on your computer. Or it's similar to ransomware where it'll lock the computer up if you don't give them a password and then your data essentially is destroyed.

The second element requires the plaintiff to demonstrate that the defendant knowingly intended to damage a protected computer through a result of a transmission. Intentional in this case is defined as performing an act deliberately, and not by accident, with a conscious purpose of causing damage.

The third element to this particular section that has to be proven is that the defendant caused damage to a protected computer. Damage is any

impairment to the integrity or availability of data, a program, a system, or information.

The fourth element is the damage occurred without authorization. This is not generally an issue as we only have to show damage without authorization. You could see in the case of Citrin that he had software that he used to deliberately and intentionally damage the data because he completely and securely erased it. He did this without authorization.

Section (a)(5)(B), the second of those two parts of the section, has three general elements: intentionally accessing a protected computer; without authorization; and, as a result of the access recklessly causing damage. Section (a)(5)(B) focuses on access that was intentional and unauthorized. Section (a)(5)(A) focuses on whether damage was intentional or unauthorized. So whether the defendant intended to cause damage is irrelevant under (a)(5)(B), you just have to show that the access was intentional and unauthorized. Citrin was prosecuted under both (a)(5)(A) and (a)(5)(B).

Section (a)(5)(C) has three general elements: to intentionally access a protected computer; without authorization; and, as a result of the access, to cause damage. Section (a)(5)(C) is similar to (a)(5)(B) in that (a)(5)(C) applies even if damage was not recklessly caused, and (a)(5)(C) applies if the defendants caused both damage and loss. Loss in this case is any relevant cost for the victim. That brings up a good point. If there is damage caused and you think the CFAA may apply, or in any case where there's a virus or denial of service or a compromise, it's very important to keep track of all the losses that are incurred by the company, both direct and indirect because of the crime. They will be used in determining the value of the things that were lost, as well as, to determine whether or not the crime is a misdemeanor or a felony. It certainly will help in the conviction of the criminal.

Trafficking in Passwords, Section (a)(6) prohibits individuals from, knowingly, and with intent to defraud, trafficking in passwords or similar

information to access a computer, without authorization, provided it affects interstate or foreign commerce or a computer used by the government. This was added in 1986 over the concern of stolen passwords being placed on "pirate bulletin boards". It shows you again how old the CFAA was, but 1996 we were still concerned about pirate bulletin boards. Today, we see the pirate bulletin boards replaced by Tor sites and other types of dark websites where you can find stolen passwords and user accounts that can be used to illegally access, without authorization, certain sites around the country. In this case, the trafficking means to transfer or otherwise to dispose of to another, or to obtain control of with the intent to transfer or dispose of. In other words you're gathering the data and you intend for it to be used by others in the furtherance of a crime. You must show an intent to defraud. It only applies if the trafficked passwords allow unauthorized access.

Section (a)(7) Threatening to Damage or Obtain (Threats of hacking). This prohibits individuals from transmitting in interstate or foreign commerce any communication containing three types of threats or demands: the threat to damage a protected computer; the threat to obtain information from a protected computer without authorization, or in excess of authorization, or to impair confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; and the demand or request for money or anything of value in relation to the damage of a protected computer where such damage was caused to facilitate the extortion. This sounds an awful lot like ransomware, doesn't it? It does not depend on the actual accessed, damaged, or obtained information. It applies only to the attempt to extort money from a victim. In the case of ransomware, they do actually damage the system, but they're still extorting money from you. I'm certain that Section (a)(7) would probably apply there.

Section (a)(7) is similar to the Hobbs Act. The Hobbs Act is a federal extortion law that imposes a fine up to 20 years in prison for threatening physical violence to any person or property. The property under the Hobbs Act does not clearly include the operation of a computer, the data, programs stored in a computer, or its peripheral equipment--decoding keys for encrypted data etc. In 1996 this section was added to address the emerging

problem of computer-age blackmail. Think about that… where was the internet in 1996? We were still very small at that point in time. I think I've seen numbers on the order of 16 - 20 million computer users at that point in time in the internet. The internet was very small but the legislators had the foresight to think that this would and could become a problem.

Ransomware, as I said, Section (a)(7), brings criminal and civil actions against hackers. The difficulty of prosecuting under Ransomware is, first of all, the anonymity of the people who are conducting the operation: the fact they're using Bitcoin for the transference of the payment, rather than sending money to a certain bank account or to a certain person; and the fact that where the crime is actually originating is more than likely outside the U.S. in foreign countries.

Most states have Anti-hacking laws similar to the CFAA. Some states predate the CFAA and some may cover many types of computer repair related actions. An example in the text is in California where there are 154 types of actions that are covered under state and computer hacking laws. The link to additional state laws is on the Learning Activities page. You can look there and see more additional information on the state law.

Unit 6

Let's continue by looking at some additional laws that protect against electronic crimes. Copyright laws have been with us since the inception of the country. These laws provide a property right to the original creators of the content of books, newspapers, music, movies, artwork, and sculpture. The material we see in written form or in physical form is protected by these copyright laws. However, as things have moved online, the copyright laws have not kept up with the types of protection needed. The Digital Millennium Copyright Act (DMCA) restricts the ability of individuals to **circumvent access controls** that protect copyrighted material. I highlighted the text "circumvent access controls" because this is a subtle point. The copyright laws protect the content; the DMCA prohibits circumventing access controls that are instituted to protect the content. Historically, we could look back to 1996. The World Intellectual Property Organization or WIPO treaty set the rules for copyright protection and required signatory countries to provide legal protection and provide remedies against those who try to circumvent the protections placed on content.

In 1998, the United States enacted the DMCA. Section 1201 punishes circumvention if the purpose of the circumvention is to break the control. There are three key provisions. Section (a)(1) prohibits the act of circumventing technology that controls access to copyrighted material. Section (a)(2) prohibits trafficking in the technology that facilitates circumvention of access control measures. Section (b)(1) prohibits trafficking in technology that facilitates circumvention of measures that protect against copyright infringement.

Let's look at Section (a)(1) that prohibits the act of circumventing technology that controls access to copyrighted material. This relies solely on whether the individual circumvented technology that was meant to protect copyrighted material. This Section does not prohibit subsequent use of the material, just the circumvention of the access control. The subsequent use is covered under the copyright laws as would be any other copyrighted content. This section is focused only on circumventing access

controls. The Courts have accepted many types of controls; in fact, even just the use of a simple password is sufficient to show that an access control exists. They don't set the bar for the sophistication of the control; the control is simply something that is protecting access.

We could look at some of the technologies that have been used over the years. Passwords, of course, but Content Scrambling System (CSS) in 1996, was also one of the early ways of protecting content, even video content on CDs and DVDs. CSS is relatively weak-a proprietary 40-bit stream cipher algorithm, and very easily compromised today. Content Protection for Recordable Media and Pre-Recorded Media (CPRM/CPPM) is again an encryption process. It's a 64-bit block cipher with a 56-bit key, and again fairly easily compromised today.

The Advanced Access Control System (AACS) with Advanced Encryption Standard (AES) uses an encryption pattern AES to protect content and is certainly a lot stronger than either CSS or CPPM. There's also what's called Regional Coding (RC) and Regional Coding Enhancement (RCE). This is applying specific regional codes and blocks access to the disk outside of your region….sort of. When I lived in Europe, I would buy a DVD in Europe, put it into my DVD player, and it would say this is outside your region. Would you like to set your player to that region? I guess there are a certain number of times you can make that switch. It's a relatively low number such as five or six times that you could change your DVD player to actually show that region. This was on my computer, not on a commercial DVD player that would play on the TV. The User Operation Prohibition (UOP) prohibits the user from skipping certain parts of a disc. That's usually where you would find the protection things such as the copyright notice and the FBI notice. Have you noticed when you start up the DVD or watch a movie that you can't skip over those sections because it's been disabled? Sony Advanced Regional Copy Control Operating Solution (ARccOS) was Sony's version of regional coding layered on top of CSS.

I've put on this slide features of a couple of software packages that are marketed today to break the access control of DVDs and even Blu-Rays. As

you can see in both cases, they do talk about having that capability to break those controls. By the way, don't do this. As you can gather from the lecture, it's pretty risky, and I'd say certainly not necessarily legal. One of the advertising aspects of some of this software is they claim you can make a copy as a backup to your DVD, should you lose your DVD.

Section (a)(1) violations do not occur merely because a user violates a user agreement. If a user agreement prohibits certain activities, that's not really covered under Section (a)(1). An example of this is Auto Inspection Services (AIS) v. Flint Auto Auctions (FAA). Flint Auto Auctions was a former customer of AIS, and they developed competing software. A developer for the Flint Auto Auctions told the court that Flint Auto Auctions provided him printouts of the AIS software interface. AIS sued for violation under Section 1201 (a)(1) and sought an injunction. The Court denied the request concluding that AIS failed to show that FAA had circumvented any technological features. Using the printout is not the same thing as accessing source code, modifying source code, or creating a derivative software program. They simply made screen printouts and were able to produce the software from there. Again, it may have been a violation under copyright, but not under Section (a)(1).

Section (a)(1) plaintiffs must allege in their complaints that a specific technology was circumvented and how that circumvention occurred. In the case of LivePerson Inc. (LP) v. 24/7 Customer Inc. (24/7), LP alleged that 24/7 had a joint agreement with LP to support some customers. LP sued 24/7 claiming the 24/7 had used its access to the software and backed in to create competing software through reverse engineering. To reverse engineer you would have to break the access control. You'd have to look at either some kind of source code or you'd have to look at disassembly language code or something to be able to reverse engineer it. The court rejected their argument stating than just because 24/7 may have mimicked LivePerson to gain access to the software components, it didn't break an access control. LP was not specific as to what access controls were circumvented or how.

Still Unit 6.

Let's complete our discussion of the DMCA by looking at Section 1201 (a)(2) which prohibits an individual from trafficking in any technology, product, service, device, or component that A) is primarily designed to circumvent a technology that effectively controls access to a copyrighted work; B) has only limited commercial significant purpose or use other than to circumvent a technological measure that effectively controls access to a copyrighted work; C) is marketed by that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work. 1201 (a)(2) is specifically focused on the trafficking of technology designed to circumvent access controls protecting a copyrighted work. if you think back on (a)(1), that was the technology itself; now we're looking at (a)(2) that we're trafficking in that technology.

The scope of 1201 (a)(2) has been interpreted both narrowly and broadly by various courts. We see this in all the electronic Crimes laws. Some Courts interpret the laws very broadly, and some interpret them very narrowly. The narrow approach in the case of 1201 (a)(2) requires that a nexus between the access that is violated and the protection of the copyrighted work exists. In other words: there is an access protection; it's broken; it's violated; and access is given to the copyrighted work. The opposing broad view applies to technology that circumvents the controls that are used to protect that copyrighted work. Regardless of whether the technology actually is used to access the copyrighted work itself, the broad view just says the technology exists, even if you can't show or don't need to show that it was actually used to circumvent some copyrighted protection. Each of these two approaches developed their own six-point test to determine if that approach should be applied.

In the Courts that use the narrow test, the plaintiff must prove that its ownership of a copyrighted work was effectively controlled by a technological measure; that third-parties can now access without authorization and in a manner that infringes a right protected by copyright. And all the above happened because of a product the defendant: A) designed or produced primarily for circumvention; B) made available

despite only for limited commercial significance other than circumvention; C) marketed for use in circumvention of the controlling technology measure. In essence, you can see here that nexus. I have a copyrighted work; it has an access control; that control has been circumvented giving access to the underlying material which infringes on my right to protect that copyrighted material.

In the broad test that's applied in some Courts, the plaintiff must prove that the defendant trafficked in a technology or part thereof, that is primarily designed, produced, or marketed for or has limited commercial significant use, other than circumventing a technological measure that effectively controls access to a copyrighted work. You can see how this is much more broadly defined. You don't have to show any circumvention took place, just that the technology was capable of circumventing the access control that protected the copyrighted material. Because of these two tests, the broad test and the narrow test, or, more importantly, the broad interpretation by Courts versus a narrow interpretation by Courts, you certainly get a feeling that either the defendant or the plaintiff is going to try to shop for certain venues that will tend to support their level of argument against the opposing side.

Section 1201 (b)(1) states that no person shall traffic in any technology that: A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects the right of a copyrighted owner; B) has only limited commercial significance; and C) is marketed by that person for use in circumventing protection afforded by the technological measure that effectively protects the right of the copyrighted owner.

Comparing Section (a)(2) with Section (b)(1), Section (a)(2) applies more broadly to the circumvention of technology, regardless of whether the circumvention aids infringement, and that (b)(1) applies more narrowly, focusing on the technology that does aid in the copyrighted infringement. So, in (a)(2) you don't have that variation that says you don't have any circumvention taking place, whereas (b)(1) is more narrow, as there must

be copyright infringement. Certain exemptions can be applied to the anti-circumvention provisions, such as making short portions of motion pictures available for criticism or comment. You see this all the time in presentations where people take a small snippet of a movie or a video and show that for a point they want to make in their presentation. I would suggest that you still cite your reference and cite the owner of the copyrighted material just to protect their right to that material. There are also some computer programs that enable smart televisions to operate and certain lawfully acquired video games that have some lawful exceptions.

The argument against the DMCA comes from those who argue that the First Amendment might apply here. That software code is speech; and, by prohibiting certain types of software code that the 1201 censors, speech is censored, and therefore this violates the First Amendment. For instance, security researchers may write code that helps them find vulnerabilities in software or protection capabilities. If the rules of the DMCA are applied, they would be fairly risk-averse to avoid civil litigation that might arise if they show that there are vulnerabilities in that software, and that the codes that they've written actually circumvent the access controls in order to prove the vulnerability of that software they are testing. There have been cases of researchers that have found flaws in copyrighted protection software who were threatened with lawsuits if they actually produced their results, made presentations on their results, published their research, etc. One case that comes to mind is Universal City Studios Inc. v. Corley. Corley published the DeCSS code on his computer hacker website 2600.com and then set up links to the host sites elsewhere in the internet. But for DeCSS, the only purpose of the code was to defeat the CSS protection on copyrighted DVD movies. Again, this was produced only for the purpose of defeating that technology, so certainly you would think that 1201 would apply in this case.

How do we analyze whether or not this is a valid First Amendment claim? Does this law regulate speech? If the law regulates speech, is the law content-based or content neutral? If it's content-based, it will only survive a First Amendment challenge if the government demonstrates that it serves compelling government interests by the least restrictive means that are available. In other words, the content of the speech or the software code

serves a compelling government interest. In most cases, if it's content-based, more than likely it won't survive that First Amendment claim. If it's content neutral, on the other hand, there's more that needs to be proven. It has to further a substantial government interest unrelated to this suppression of free speech and the laws narrowly tailored so it does not burden more free speech than necessary. To be content-neutral, certainly it has to meet a higher bar to show that there's a violation of the First Amendment that could be applied here.

Unit 6—Part 3

Let's finish up this unit by looking at the Economic Espionage Act. This prohibits theft of a U.S. company's trade secrets to either benefit a foreign government or to economically benefit anyone other than the owner. It was passed in 1996 and amended in 2016. We'll look at those 2016 amendments to show how a company can now bring a civil lawsuit against the individual or company that conducted the trade secret theft. There are two corresponding sections to the law: Section 1831, Economic espionage; and Section 1832, Theft of trade secrets.

Section 1831: Economic Espionage. It prohibits individuals from stealing, copying, receiving, or possessing trade secrets without authorization, if individuals intended or knew that the offense would benefit any foreign government, foreign instrumentality or a foreign agent. Foreign instrumentality refers to a government agency rather than an individual in the government itself.

Section 1832: Theft of Trade Secrets. It prohibits individuals from stealing, copying, receiving, or possessing trade secrets without authorization, if the individuals acted with the intent to convert a trade secret related to a product or service used in interstate or foreign commerce to the economic benefit of anyone other than the trade secret's owner. Basically, you have a theft of a trade secret which is provided to someone else, other than the trade secret's owner, and so that someone else can reap the economic benefit of it. We see this a lot in industrial espionage where someone will steal a trade secret and sell it to another company, perhaps in another country, so that that company can avoid the R&D cost necessary to develop and compete on a particular product. Certainly, the economic benefit will go to that other company and possibly to the individual who stole the material, and, certainly, that would impact the economic value of the product to the original owner and designer of the product.

Section 1836: Civil Actions was added in 2016. This allows the victims of trade secret misappropriation to file civil lawsuits, seek injunctive relief, and seek monetary damages for trade secret theft.

The differences between Sections 1831 and 1832 are based on the purpose and intent of the defendant's trade secret theft. It requires the defendant to have done one of five acts: stealing, or without authorization, appropriating a trade secret; making a copy, without authorization, of that trade secret by any number of a different ways as shown on the slide; receiving, buying, or possessing a trade secret, with the knowledge that the trade secrets were stolen or appropriated, obtained, or converted without authorization; attempting to commit any of the above acts; conspiring with at least one other person to commit any of the first three offences, and one or more of the conspirators effects the object of the conspiracy. So, you don't have to be the one who actually steals the trade secret. If you conspire with at least one other person and that person steals the trade secret, then under this law you are as guilty as the person who conducted the theft.

What is a "trade secret" ? Think about the things that your company does that are very important to the company; many of those things might be considered trade secrets. Here are some examples: financial information or business decisions; companies you want to buy or sell; actions a company might take that could impact either positively or negatively the value of the company; its scientific developments; patents, of course; technological designs; and architectural designs. Anything that brings value to your company-whether it's physical, electronic, graphical, photographic or just in writing could be considered a trade secret. But for it to be a trade secret, you also have to take reasonable measures to keep such information secret. For instance, let's say I have a really great design for a widget, and I know I can earn a lot of money selling this widget by putting it on the market. And for some reason, I put this on the Internet to show everybody that I've designed this widget: here's how I've designed it, and it's the greatest thing since sliced bread. Now I'm looking for funding and would certainly like some funding from everybody because you can get as big a piece of this pie as I'm going to make. Well then, you probably haven't taken the measure to keep that widget information secret, and it certainly would be difficult to prove that it is a "trade secret" for you. The information needs to derive independent economic value, actual or

potential, from not being generally known to the public or readily accessible through proper means by another person who could obtain economic value from the disclosure of that information. A trade secret has to be a secret for it to be a trade secret!

Protecting trade secrets from internal users means the trade secret should be on a need-to-know basis. Not everybody has to have access to the designs. A person who does Human Resources doesn't need to see the confidential design for a new product. They may certainly be involved in the hiring and firing and actions of individuals who work in that department; but, they may not need to see the actual product designs themselves or the code that's behind a software product, etc. To prevent employees and outsiders from stealing trade secrets, there are some things that a company can do that can help protect those trade secrets. One is to require every employee to sign a confidentiality agreement. If an employee leaves your company and goes to another company, the confidentiality agreement may protect your company, should that individual tell other people how the product is designed, or how to use your firewalls, intrusion detection software, strong passwords, layered protection between the internet and the intranet and storage locations. So, think of those concepts of defense in depth and have as many different items as you can that will protect your network and your store of knowledge and trade secrets that are on the network. Another thing that you can do, which I've seen used in a lot in companies, is to segment your network. Trade secrets are kept on a separate network that can be access-controlled at the network level to begin with and then at the individual level, or a cap level, when you get closer to the trade secrets. Use non-disclosure agreements when sharing information outside the organization. Mark documents as confidential; rarely do I see this taking place. Mark the documents as confidential or as restricted, or whatever you apply to your definition of protecting your trade secrets. With this protection in place, an individual who has a copy of your document can clearly see that the document is not meant to be shared outside your organization. Put that classification system into your information security policy and train individuals to mark the documents and understand what the marking of documents means. Strengthen the physical security of your facilities. Don't allow terminating employees to have access to computers without supervision. In the exit interview, review the non-

disclosure and confidentiality agreements with the terminating employee, so that they understand what their obligations are as they leave the company.

Unit 7 Part 1

Public and Private Collaboration is a simple concept that's difficult to accomplish. We saw in PDD63 that we established a concept of sharing information and intelligence. What are the problems that we're seeing? Well certainly, anonymizing the data to protect privacy is especially important. People tend to want to share data, if other people don't know it came from them. How do I get my information from me to another person or another agency that's trying to protect the information? There is reluctance on the part of private companies to participate and difficulty in sharing by organizations on the public sector-side. Around 2015, the practice started to come together. But we still see numerous agencies responsible for cyber security. For instance, at the FBI there's the InfraGard Internet Crimes Complaint Center and the National Cyber Forensics and Training Alliance; in the Secret Service we have the Electronic Crimes Task Force; in the Department of Defense we have Cyber Command; in the Department of Homeland Security we have the Office of Cybersecurity and Communications; at the U.S. Justice Department we have Computer Crimes and the Intellectual Property Section; in the U.S. Department of Commerce we have the National Institutes of Standards and Technology; and even the U.S. Energy Department is involved in the process with their CRISP program. The point is there are many different voices that need to be heard, and it's difficult to effectively bring all those voices together from the public sector to communicate threats to the private sector.

The National Cybersecurity and Communications Integration Center (NCCIC) encompasses the U.S. Computer Emergency Readiness Team or the U.S. CERT, which provides a 24-hour monitoring of emerging cyber threats and communicates these out to the subscribers regarding the observed threats. Under the Cybersecurity Act of 2015, the DHS has assumed the central role in coordinating cybersecurity monitoring and alerting. They've encouraged the private sector to participate and provided limited legal immunity to private sector companies reporting events. They've expanded the role of the NCCIC and assigned the responsibility of cybersecurity planning to the NCCIC and DHS. Many of the agencies that I

listed in the earlier slide have a seat at the NCCIC to help coordinate cybersecurity activity that they observe.

Private industry has been reluctant to share information with the public sector. Probably the most compelling reason that we see for a company's reluctance is the fact that participating in a sharing process could impose a liability on the company. If they spot something, or someone else spots something, and you see it, does the fact that you have knowledge that a threat exists impose a duty upon you to act against that threat? That's the question that needs to be answered under that particular aspect of reluctance. There could be antitrust issues. Certainly, this was a question that was presented as the ISACs (Information Sharing and Analysis Center) were developed, for instance, the FS-ISAC, or others. When you're thinking of bringing all these companies together to share threat data, you must be careful not to walk over the line and create an antitrust scenario. When you attend ISAC meetings, very seldom will you hear anyone mention products or various products in the marketplace because that could create that antitrust scenario. Certainly, another question is violation of privacy, should you expose private information in the process of sharing. However, the Cybersecurity Act of 2015 creates new processes for companies to monitor and defend their networks. It creates a new platform for the exchange of information between the public and private sectors such as cybersecurity indicators and defensive measures.

Limited liability or limited immunity applies to the sharing of cybersecurity indicators and defensive measures. These indicators are the information used to describe or identify certain types of acts, such as: malicious reconnaissance; methods of defeating a security control; exploitation of security vulnerabilities; identification of security vulnerabilities; phishing; malicious cyber command and control; networks that are being set up; actual or potential harm caused by an incident including exfiltrating information; or other attributes of a cyber security threat.

Some of the threat indicators that you might share, or we do share, are things such as: IP addresses with malicious URLs and log extracts showing

failed attempts to log into users' accounts. You don't want to show the user's name, but you can show the data associated with the individual or party that's trying to make those login attempts. Another threat indicator is log extracts showing successful login to a user's account at a time when a user wouldn't normally log into the system. Certainly again, you wouldn't want to share the login information, but you could share the indicators that surround that particular episode. Threat indicators to share also include domain names associated with malicious or suspicious activity. We call these "use cases" when we're using them to design defensive measures, for instance, with our security event monitors, our firewalls, and intrusion detection and prevention systems. We build out what we call "use cases" or examples of things that we want to block with a particular rule or for which we want to establish a monitoring pattern.

Defensive measures are actions, devices, procedures, signatures, techniques, or other measures applied to an information system or to information that is stored on a system which prevents or mitigates known or suspected threats or security vulnerabilities. Defensive measures expressly do not include measures that destroy, render unusable, provide unauthorized access to, or substantially harm an information system with information stored on, or processed by, or transiting on a system not owned by the private entity operating the defensive measure or another entity acting on its behalf. In essence, defensive measures are processes that allow you to detect, prevent, or mitigate known or suspected threats, but without harming the computers that are generating the threat. You see laws occasionally pop up in in the Congress for active defense measures. Basically, they are allowing you to go out and analyze where threat activity is coming from. In all these laws that I've looked at, there are very specific protections and warnings against harming the other computers that you may be looking at, even if it is the person's computer in another country who executed the threat directly against you. You must be incredibly careful if you're looking at active defense measures.

As stated, the cybersecurity Act of 2015 provides limited legal immunity for companies that share information to the public sector. If a company complies with the provisions of the Act, it will not be held liable for monitoring its systems for cyber

threats or properly sharing and receiving cyber threat indicators. However, immunity only applies if sharing information for cybersecurity purposes. A cybersecurity purpose is the protection of an information system, or information stored on a process, from a cybersecurity threat or security vulnerability.

A cybersecurity threat can be an action not protected by the First Amendment on or through an information system. It may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or the information stored on, or processed by, or transiting a system. A cybersecurity threat does not include a violation of the customer terms of service or licensing agreement. The companies cannot gather and share private information with the government. You cannot share things like credit card data or the banking information. You must be careful about sharing even an individual's name or any other confidential information that you may store as a process of your business. Talk with your legal counsel to ensure that what you are sharing is not considered private information that you would be passing on to the government.

There are caveats to limited immunity. You must comply with DHS procedures, prevent information from unauthorized access, review cybersecurity threat indicators before sharing them out to ensure that what you have really are threat indicators, and remove any information that's not directly related to that cybersecurity threat. Most importantly, the Cybersecurity Act of 2015 does not create a duty to act. The private sector can use the shared information to affect the security change or not. The private sector is not required to share cyber threat information or use the information that they receive. It's up to them. The DHS created the automated indicator sharing system for sharing and receiving cyber threat indicators, but this is still gaining ground and is not what we normally see in the process of sharing data at this point.

The Energy Department also has cyber threat information that it can share, and certainly would like to receive information from companies that are in the energy utilities business. There's a serious threat to national security if

the electric grid is disrupted. You can imagine some of the risks if you think about the loss of power in 2013, up in the Northeast. That caused a massive amount of economic impact for a very short 29-hour outage. So, imagine that if there were a much more damaging attack on the power grid, there could be a serious economic, as well as a national security impact on the country. In 2013 the U.S. Department of Energy developed the CRISP program (Cybersecurity Risk Information Sharing). It's a voluntary program for sharing classified and non-classified cyber threat data with the Energy Department as an intermediary. The Department of Energy recognized cyber threats for their disruptive potential and put this program together so that they could share and receive data from the various utility companies.

Unit 7, part 2

We talked about active defense in the last part of this unit, and I want to talk a little bit more about some of this activity. We're seeing legislation being proposed periodically that would allow companies to take what they call an active defense posture. One such bill, H.R. 3270, was introduced into the House of Representatives on June 13, 2019. It was an effort led by representative Garret Graves, a Republican from the 6th District in Louisiana. It was similar to a bill that he had proposed in 2017, but this particular version of the bill has bi-partisan support.

The bill recognizes several basic premises concerning cyber fraud and cyber enabled crimes that pose a severe threat to the national security and economic viability of the United States. It's difficult for law enforcement to respond to and prosecute cybercrime on a timely basis, and this leads to a low-level of deterrence in a rapidly growing threat. The criminals know that the odds of them being caught are fairly slim. Even if they are caught prosecution is even more difficult. Cyber criminals have developed new tactics for monetizing the proceeds of their crimes and that further incentivizes their activity. There's a general lack of the cyber tools and deterrent methods that defenders can use to protect themselves. Even where those tools may exist, you may find that the defense of a particular company is really dependent upon the approach of the company itself in its ability to spend money and find the talent to protect its operations. Let’s face it: victims in the U.S. tend to report crimes to law enforcement, if they report them at all.

Cyber-attacks would be prevented through improved cyber defense practices, and, hence, training, stronger passwords, routine updating and patching. These things need to be in place before you think of doing anything else, and, in particular, you need active defense processes. Without having the fundamentals in place, taking additional action is just a time-consuming process. Congress determined that the use of active cyber defense techniques, when properly applied, could assist in improving defenses and deterring cybercrimes.

There's an increased interest among the private entities to stem the growth of the dark web in order to return private property, intellectual property that's been stolen from them, and financial records that they may have had the responsibility of protecting. The Department of Justice needs to clarify what some of the proper protocols are for the entities pursuing active cyber defenses in the dark web. Federal agencies need to prioritize cyber incidents of national significance, and computer defenders should be cautious to not violate the laws of other nations where the attacker’s computer may reside. Now that statement alone implies that you understand the laws of other nations. If you do not, then you will need legal support to make you aware of those laws. You don't want to end up violating those laws and causing yourself more grief.

Only qualified active cyber defenders should conduct this practice. The question is, what is a qualified active cyber defender? Is that a certified ethical hacker? Is that a person who has practiced cybersecurity activities for a certain number of years? Is it somebody who specializes in firewall technology? What is it that makes a qualified active cyber defender? Who

determines that? Only a qualified active cyber defender should conduct this practice when there's a high degree of attributional confidence. Extreme caution should be exercised to prevent impacting intermediary computers and creating an escalatory cycle of cyber activity. If you can imagine that if you do not properly protect your identity when you're actively defending your system in the dark web or on an intermediary computer, then you could end up creating a blowback where the people start attacking your company. Specifically. Particularly with a probable denial of service attack that could devastate your ability to operate. The Act was specifically designed to provide legal certainty, such as clarifying tools and techniques that can be used and the allowance to exceed the boundaries of your own network. This Act would modify Title 18 U.S.C. Section 1030, of which we looked at much earlier, the CFAA.

Section 1030 would not apply to those who use attributional tools which are programs, code, or command for attributional purposes. Attributional tools, in this case, just means the tools allowing us to understand who the attacker is—for example, beacons that return a location or metadata, in response to a cyber intrusion. The kicker here is that the attributional tools must be loaded on your defender's network (your network) and copied or removed by the attacker. You don't go out and put the material out on their systems. It has to be removed by them. It's important that the tools cannot destroy any data, even the attacker's data, or result in the impairment of the operating system on the attacker's computer. When people think about active cyber defense, they believe they can just go out there, get access to the attacker's computer, and then blow away his computer! Just as the cyber attackers have done to us! Well, you can't do that under this law. Also, you would be creating a backdoor or providing

intrusive access into the attacker's computer system which is forbidden. So again, attributional data is digital information, log files, text strings, time stamps, malware samples, IP addresses, and digital artifacts that can be gathered through a forensic process and that help to identify the location or an additional location, if the attackers use a proxy computer to attack you. You also have an exclusion from prosecution. It's a defense from prosecution that the activity was an act of a cyber defense measure. It does not prevent a U.S. person or entity who was the target of this activity from seeking civil remedy. If you can identify the attacker through these attributional activities, you may seek compensatory damages or injunctive relief.

Active cyber defense does not include conduct that intentionally destroys or renders inoperable information that does not belong to the victim, stored on another person's computer. You could destroy your data, but you could not destroy any other data that's out there. For instance, if you're out on a site and you see a lot of credit card data and you can identify that which was stolen from you, can delete that data but you can't delete the rest of the data that's out there. You cannot recklessly cause physical damage, injury, or financial loss. You cannot create a threat to public health or safety. You cannot intentionally exceed a level of activity required to perform reconnaissance on an intermediary computer, or to determine attribution of the origin. It's rather interesting that you cannot exceed the level activity required to perform reconnaissance on an intermediary computer. Does that mean you can access the computer, but you cannot do anything more to it other than to look through the log files perhaps? Or possibly gather some information that may help point you to another computer? But, by reference, the law seems to allow you to gain access to

an intermediary computer, which may certainly be somebody else's computer out on the network, another individual, or another company. I would get legal advice before attempting to access an intermediary computer. It does not allow conduct that intentionally results in persistent disruption of a person's internet connectivity, so that you are not allowed to figure out where the attacker's computer is and do a denial-of-service attack for instance. You cannot impact any government computers involved in the administration of justice national defense or national security. If the intermediary computer happens to be, let's say in the NSA, you probably don't want to actively engage in any activity on that computer.

The Notification Requirement is that the defender must notify the FBI National Cyber Investigation Joint Task Force AND receive a response acknowledging receipt of the notification BEFORE using the measure. You need to provide to the National Cyber Investigation Joint Task Force the type of cyber breach that occurred, the intended target of the active cyber defense measure, the steps that you intend to take to preserve evidence of the attacker's criminal cyber intrusion, and the steps to prevent damage to intermediary computers not under ownership of you, or the attacker.

Again, it's a proposed law. We'll see if it goes anywhere. If a law on active cyber defense ever does come into play, make sure you have legal advice before you engage in anything that can impact an intermediate computer or the attacker's computer.

Unit 7, part 3

There are several security frameworks that a company could use in defining their security compliance and privacy policies. Certainly ISO 27001 and ISO 27002 are used by a number of companies to help promote their security practices. NIST Special Publication (SP) 800-53 and SP 800-53 are a joint audit program and have been used for a number of years by federal contractors and government agencies to establish the security practices that protect their enterprises. Importantly, the NIST Cybersecurity Framework that we're looking at here, as well as ISO 27001/27002, and the NIST SP 800-53, provide a tremendous number of security practices that you should consider putting into place to secure your enterprise. However, even though these have been around for a number of years, many companies still haven't developed a security plan to protect their enterprises…or the security plan that they have in place is not sufficient. There are too many gaps in the types of practices that they should conduct. This is concerning particularly if companies are part of the critical infrastructure. President Obama signed an executive order defining a national policy to enhance security and resilience in the national infrastructure.

The Executive Order encouraged efficiency, innovation, economic prosperity and promoted safety, security, business confidentiality, privacy and civil liberties. At the same time, it created a partnership between the public and private sectors. It did not call for new regulations; but it did call for the Attorney General, DHS, and the Director of National Intelligence to develop practices for sharing information. It also directed NIST to develop a voluntary framework.

The Cybersecurity Framework draws upon existing security practices. It's not a one-size-fits-all framework. We'll look at that in a few minutes. Many firms, large and small, are adopting the framework. No matter which framework you review, basically, there are five key principles for cybersecurity risk management that you'll want to focus on when you're designing your security policy: 1) Identify 2) Protect 3) Detect 4) Respond and 5) Recover. If you think about it, this is the cycle you would use in

cyber defense: identify a problem; protect your company from that problem attacking you; detect it; respond to it; and recover. If we look at each of those elements inside the NIST cybersecurity framework, you need a checklist of things to have in place in your cybersecurity plans.

In the Identify principle: understand the organization and cybersecurity risks to systems, assets, data, and capabilities. Inventory your applications, hardware, and identify your sensitive data. Essentially, you want to identify what it is that you're protecting. Map your organizational communications and data flows so that you understand how they properly flow. Prioritize assets as to criticality and business values. Which assets are the most critical to your operation and have the most business-value to your operation and which are less critical? Identify and address cybersecurity risks. Establish cybersecurity roles and responsibilities. Establish business functions for the delivery of critical services. Establish resilience requirements. What is it that you need to have in place, so that critical assets can be brought up as quickly as possible? What are the requirements for your response in a critical situation? Understand and manage legal and regulatory requirements including privacy, and document and identify a set of vulnerabilities.

In the Protect principle: Implement safeguards to deliver services. What is it that you want to put in place to protect your infrastructure? Manage identities and credentials for authorization and access to accounts and devices. A critical aspect of protecting your network is knowing who should be on the network, who's authorized to be on the network, and making sure that those credentials are kept up to date when an individual leaves the company. What are your policies and procedures in removing that individual’s access? Incorporate network segmentation; inform and train all users, particularly privileged users and senior executives. Security awareness is a requirement for many compliance obligations. It's important that people understand the security that is on your network, and how they are part of it.

Protect Data, at rest, in transit, and during processing: Implement data leakage protection. Data leakage is simply how data can leave your

company from different areas, such as being emailed out by a customer service representative who's trying to communicate with a client, or that credit card data is being sent out by email from one company department to another company department, and it's not encrypted etc.. Formally manage assets throughout removal transfers and dispositions. Separate testing and development networks from production networks. This is critical. Typically, we have less security restriction in the testing and development networks. They should be separated from the production networks so that you have no crossover from those less protected areas into your live data. Establish a software development lifecycle and establish a change control process. Change control processes are especially important in a company to be able to understand the impact of changes on your network, and to give people an opportunity to see what changes are taking place. Establish and test your backups. Develop and review the audit logs.

In the Detect principle - Continuously monitor the organization's systems and networks to quickly become aware of incidents. Analyze detected events to understand attack targets and methods. Aggregate and correlate event data from multiple sources. Determine the impact of events and establish alert thresholds. We tend to have so many alerts that pop up that are either false positives or are only common activity that really has no impact on the security of your network. You want to be able to set those thresholds so that you see the things that are important to see as you go day to day on reviewing your network and not be bogged down by the less important material. Detect malicious code and unauthorized mobile code. Perform vulnerability scans. When you perform vulnerability scans, ensure that you set-up mitigation plans and have individuals assigned to those plans with dates when issues will be corrected. Test detection processes, communicate event detection information to appropriate parties, and continuously improve detection processes.

In the Respond principle - Develop and implement a cybersecurity Incident Response Program: execute your response plan after an event; report events consistent with established criteria; share information consistent with response plans; coordinate with your stakeholders;

understand the impact of an incident; perform forensics. Performing forensics doesn't necessarily mean you perform the forensics unless you are trained as a forensics specialist and have the capability in your company to do a forensic examination properly. Properly means all the way from acquisition of the data through the preservation of the data after the investigation is completed. It's not as simple as it sounds to conduct a proper forensic investigation, so that should be left to experts. Categorize incidents consistent with response plans. Contain and mitigate incidents. Mitigate and document newly identified vulnerabilities and their accepted risks. Finally, incorporate lessons learned into response plans and update response plans.

In the final principle of the Cybersecurity Framework--Recover - Develop and implement a plan to restore networks and systems after a cyber security incident. Execute a recovery plan during and after an event. One of the things to keep in mind with recovery plans, is, as they are being developed, you should test them, train on them, and ensure the people who need to respond understand their responsibilities before you have to actually execute your recovery plan. Manage public relations; repair your reputation after the event. Communicate recovery activities to internal stakeholders like the executive and the management teams. Continue to incorporate the lessons learned into the response plans and update your plans as needed.

Again, the NIST cybersecurity framework is not a one-size-fits-all strategy. That's a lot! We looked at all those activities, and, for a small company or a company without a lot of security resources, that's a lot to do to ensure that your company is safe.

The NIST framework looks at what they call Implementation Tiers. These Tiers are based upon the company's rigor and sophistication, and quite frankly, its budget to be able to implement all of the actions in the NIST Cybersecurity Framework. Risk Tier 1 is considered Partial. In other words, you don't have the full plan into effect. The risk management process is not formalized, and it's managed on an ad-hoc basis. The integrated risk management program has limited awareness of the

cybersecurity risk at the organizational level and the risk awareness process has not been established or is, at best, irregular. External participation, the processes and practices are not in place to work with other entities on the cybersecurity practices. You may think only smaller firms are considered Tier 1, but there are larger firms that have insufficient practices to protect themselves. More importantly, companies may have insufficiently designed practices to protect themselves, which may very well still have them down in Tier 1 level. How does one determine if they're in this Tier? You can look at all of those cybersecurity activities that we listed for the NIST security framework and check off which ones you have put into place. You're basically doing a gap analysis and then determining what else you could put into place.

Risk Tier 2 is Risk Informed. The risk management processes are defined but not fully implemented across the organization. You do have some risk prioritization. The integrated risk management program shows an awareness of cybersecurity risk at this organizational level, but there's not an organization-wide approach to managing those risks. You are risk-informed, and you've developed a process of some procedures, and, as these are approved, they're defined and executed. The cybersecurity information is shared with the organization. External participation is a bit above Tier 1. You're aware of your role in the larger ecosystem but you're not executing processes in a formal way to share that information externally. How do you move from Tier 1 to Tier 2? That goes back to understanding the gaps and executing from there.

In Risk Tier 3, we have the risk management processes defined and expressed in policy and regularly updated; risk prioritization is adjusted for changes and business requirements and threats; your integrated risk management program shows an organization-wide approach to managing cyber risk; you have risk-informed policies and processes; things are implemented as intended and reviewed; and you have consistent methods in place to respond effectively to changes in risk. With external participation, you understand your dependencies on partners and it enables collaboration and risk-based decisions to events. Imagine what you need to do to move from risk Tier 2 to risk Tier 3.

Risk Tier 4 is Adaptive. Your risk processes adapt to security practices based on lessons learned; you have continuous improvement, and active adaptation to evolving threats; your integrated risk management program is organization-wide; you have risk informed policies and practices; cybersecurity risk management is part of the organizational culture; and you share data and risks with partners to ensure accurate current information is distributed before an event occurs. The question becomes--is it necessary to move from Tier 3 to Tier 4? You'd have to look at the cost, the budget, and the organizational resources necessary to do that.

The last point is that the NIST cybersecurity framework is voluntary. But that framework is becoming a de facto standard of care for companies. Government organizations have integrated the framework into their operations. I know a number of exceptionally large companies in New York that do use the NIST cybersecurity framework, as opposed to say ISO 27001 or NIST 800-53.

Unit 7, part 4

As one last topic, let's look at the experts that we have in cybersecurity, that are members of our military. In fact, some of the finest experts in cybersecurity are members of our military. However, they are restricted from helping civilian organizations. Let’s look at some of the organizations.

The National Security Agency is an expert at signals intelligence. They employ the world's leading code breakers and are experts at the interception and deciphering of foreign intelligence operations. They operate the Information Assurance Directorate, which is charged with protecting the security of national security information. They publish advisories, guidance, and best practices for cybersecurity professionals. They develop the next generation of cybersecurity professionals with programs such as the NSA Cyber Exercise and the Centers of Academic Excellence in Cybersecurity. The University of Dallas was one of the earliest recipients of the Center of Academic Excellence in Cybersecurity.

The U.S. Cyber Command is charged with leading the Defense Department's defense of its infrastructure. It conducts its operations on behalf of the military and each of the military branches have Cyber Commands which participate in the US Cyber Command. You have the Army Cyber Command, the Fleet Cyber Command for the Navy Air Force Cyber Command, and the Marine Forces Cyber Command.

The mission of the U.S. Cyber Command is to protect the U.S. homeland and the U.S. national interest against cyberattacks of significant consequence. In order to deter those cyber-attacks, the Defense Department states that it must work with interagency partners, the private sector, and allied and partner nations. Again, the Defense Department has a deep expertise in cyber, but limitations have been placed on their ability to assist the private industry.

The Posse Comitatus Act was passed in 1878. 1878 was a much different world than we have today. The law still applies and is important in its application today. It prohibits the use of the US military to enforce laws. It does not apply to the state National Guard forces or to the U.S. Coast Guard. The military cyber operations that enforce domestic laws must fall under another statute that provides for an exception to the Posse Comitatus. The exceptions are exceedingly rare instances where this would apply. In September 2015, the Defense Department addressed the types

of cyber incidents that might allow US military to provide domestic government agencies with support. If you think of it, they provide information to the domestic government agencies, and, then, through public-private partnerships, that information might be shared to the private industry. They support remediation, restoration, and protection of critical emergency telecommunications networks and infrastructure, should there be an incident.

This wraps up the unit on Public and Private sharing of critical infrastructure data.

Unit 8, part 1

The United States Constitution is the foundational document to the legal framework in the U.S. It was adopted on September 17, 1787 and lays out the Tricameral bodies of the U.S. government. It sets up the Legislative Branch which is our Congress and U.S. House of Representatives. It lays out the Executive Branch which is the President, his cabinet, and governmental organizations like the Department of Justice., etc. The third branch of our U.S. is the Judiciary Branch-the Supreme Court.

The United States Constitution established a federal system of government. That means it reserved significant rights for the individual states, but each state had to ratify the Constitution before it was actually adopted. Basically, those powers which are explicitly in the Constitution belong to the federal government system and those that are not specifically delineated in the Constitution revert back to the states. The Constitution has been the subject of a great deal of debate even before its inception. If you go out to the website for the Avalon project at Yale School, you'll see the debate in the Federal Convention of 1787. It's actually an amazing set of documents to read and understand all of the anguish and the questioning and pulling together of different positions into one body to establish the Constitution.

Even after that fantastic Constitution was written, there were some things that were left out, and there was a lot of argument among the delegates as to the addition of some of these other rights. The first ten amendments to the Congress were adopted in 1789, and they're collectively called our Bill of Rights.

Let's look at each one of these Amendments in the Bill of Rights. The First Amendment guarantees the freedom of religion, freedom of speech, freedom of press, freedom of assembly, and freedom of petition. These are things that you see and hear about in the news virtually every day. The Second Amendment is the right of states to keep and maintain militias and the right of individuals to possess firearms. There is a lot of controversy over that amendment. You don't hear about much about the Third

Amendment, but if you search hard enough you can find cases that pertain to the Third Amendment which prohibits the government from using private houses as quarters for soldiers during peacetime without the consent of the owners.

The Fourth Amendment protects against searches, arrests, seizures of property without a specific warrant or probable cause. The Fifth Amendment forbids trial for a major crime without an indictment by a grand jury, prohibits double jeopardy, except in certain limited circumstances, and forbids punishment without due process. It also provides that an accused person may not be compelled to testify against himself. You've heard about this a lot in trials where individuals would take the Fifth Amendment so as not to incriminate themselves in a trial. The Sixth Amendment guarantees the right to a speedy trial, a right to counsel, and a right to trial by jury and due process.

The Seventh Amendment assures trial by jury in civil actions. The Eighth Amendment forbids excessive fines and bails and cruel and unusual punishment. The Ninth Amendment designates that rights enumerated in the Constitution are not all inclusive and those not specifically identified are retained elsewhere by the people.

The Tenth Amendment indicates that the powers that the Constitution does not delegate to the United States and does not prohibit the states from exercising are reserved to the States respectively, or to the people.

I'd like to take an in-depth look at the Fourth Amendment. "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the person or things to be seized." We'll look at the Fourth Amendment in both its cyber and non-cyber perspectives, but it certainly is something that has a very definite cyber impact on you, depending upon how you react to

requests from law enforcement for evidence. We'll look at this and break it down and get a better understanding of probably one of the more complex amendments in the Constitution.

Unit 8, part 2

Neither the Fourth Amendment, nor any of the other amendments that comprise the Bill of Rights, were actually developed at the time of the writing of the Constitution. There was a period of time where the founders argued about these rights and whether or not they should be included in the Constitution. James Madison proposed the Bill of Rights, but it would again take some time before there was some agreement. One could argue that the wrongs addressed by the Fourth Amendment had directly contributed to the American Revolution.

The roots of the Fourth Amendment date back to issues in England in the mid-16th century. We'll focus on the colonies rather than looking at this from a full perspective of English history. The Fourth Amendment would not have been possible but for the British legal theory which the colonial Americans of British heritage cherished as their own. We had a strong feeling of being British in the 1750's and 1760's. It wasn't as if we were rebellious from day one. There was a feeling that we were part of the motherland.

The Writs of Assistance was a type of general warrant and relied upon by the King's Customs Office and the Exchequer to ensure the collection of revenue. Officers could search wherever they wanted and seize whatever they wanted with few exceptions. A judicial official, presented with a writ, did not question it. One of the unique characteristics of these writs was that writs were valid for six months after the death of the sovereign. That's an important point which we'll be discussing shortly.

Parliament authorized these writs in 1662, empowering the Court of the Exchequer to issue: "a writ to a custom official who, with the assistance of a constable, could enter any house, shop, cellar, warehouse, room, or other place; and, in case of resistance, could break open doors, chests, trunks, and other packages, and seize any uncustomed goods."

When the writs were first applied to the colonies in 1696, they were really only applied to the Massachusetts and the New Hampshire colonies, which were under the jurisdiction of the Court of the Exchequer. The other colonies were either ignored or the issuance of writs was indefinitely delayed, or they were beyond the reach of the Court of the Exchequer.

As I said earlier, the Writs of Assistance would be in force until six months after the passing of the monarch in England. In 1760, George II passed away on the 25th of October, and the writs in existence at that point in time were technically in effect for six months after his passing before they would expire in April 1761.

James Otis, who you can see is a fine-looking young fellow, argued against the Writs of Assistance in what was called the Paxton Case. Paxton was a Custom's official. Otis's argument was that the only legal writ was a special warrant directed to special officers and was to search certain houses especially set forth in the writ that may be granted upon an oath made by the person who asked for the warrant because he suspects such goods to be concealed in those very places he desires to search. The wording there is similar, if you think about it, to the wording of the Fourth Amendment today. Interestingly enough, Otis eventually lost the case, but the point was made. We should not have searches and seizures, except that they are very specialized, and should very specifically point at designated places and persons to be searched.

The Townsend Acts of 1767 established a duty on imports into the colonies and reaffirmed those Writs of Assistance. It's not as if the Colonies, at that point in time, were being good "little angels" either. There was a lot of smuggling, outright theft of British goods, things were stolen off ships and out of storehouses, and so it wasn't like we were being good British citizens. Often when goods were seized by Custom's officials, the colonists would steal the goods back again. It was a repetitive process. Also, just as likely, the colonists would barricade themselves into their homes and hold off the customs officials and military, until the mobs joined in. Then of

course, the customs officials and the military would back away and allow the colonists to keep the goods.

There was a young attorney present at the hearing of the Paxton case in 1761, named John Adams. The case against the Writs of Assistance played an important part in John Adams's development as a revolutionary. On the night before the Declaration of Independence, Adams asserted that he considered "the argument concerning the Writs of Assistance… as the commencement of the controversy between Great Britain and America."

Many of the new states enacted their own versions of the Bill of Rights prior to those amendments to the Constitution, but James Madison who had been sort of an opponent to the Bill of Rights became then a strong proponent for them. He's now known historically as the Father of the Bill of Rights. The Bill of Rights including the Fourth Amendment in it were proposed in 1789, and, because each of the states had to vote on the Amendments, they became effective in 1791.

So, repeating the Fourth Amendment: "The right of the people to be secured and their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated and no warrants shall issue but upon probable cause supported by oath and affirmation and particularly describing the place to be searched and the person and things to be seized." Doesn't that echo the arguments that John Otis made in the in the Paxton case?

When you look at the Fourth Amendment in in a historical perspective… in fact, if you look at any of the first ten amendments in the Bill of Rights, you can see from a historical perspective how they were developed. They all had a reflection back into the history around the American Revolution in the period just prior to the American Revolution. How's the Fourth Amendment used today? What is its significance in the world of compliance and security? Most importantly, how does the Fourth Amendment influence how we establish our security and compliance programs today?

Unit 8, part 3

Let's break down the Fourth Amendment into two clauses. The first clause is that the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated. In the second clause no warrant shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized. If you look at the first clause, the emphasis is on the search and seizures. The second clause focuses upon issuing a warrant, and it states that upon probable cause, that the warrant has to be sworn to by the law enforcement officer, and it has to be very particular in its place or person to be searched or seized.

There's a tremendous amount of case law regarding what constitutes a reasonable search and seizure and when warrants need to be issued. A point to make that many people don't understand is that the Fourth Amendment only applies to government agents. It doesn't apply to corporations or individuals. It also does not provide a guarantee from the actions of a private citizen or a non-government entity based upon the conduct of a defendant. In fact, until recently, it only applied to the federal government and not to state governments. However, we'll look at Mapp v. Ohio shortly, and that's when that concept changed. A second point is that the Fourth Amendment applies to criminal law, and not to civil law. It's fundamental to criminal laws, and of course, the criminal laws are executed by government agents.

What makes the Fourth Amendment interpretation so difficult is its complications. For instance, you can have searches and seizures that violate the Fourth Amendment, even if supported by probable cause and narrowly defined warrants. Likewise, you can have legitimate warrantless searches. The first clause points to the reasonableness of searches and seizures. Fundamentally, U.S. citizens have a guarantee of a reasonable expectation of privacy, in general. This reasonableness helps us define when a search has taken place.

When we look at searches, look at Katz v. United States. The government action must contravene an individual's actual subjective expectation of privacy. The court said that the expectation of privacy must be reasonable, and in the sense that society in general would recognize it as such. For a warrant to be issued the Fourth Amendment prescribes certain elements, and that was shown in the second clause of the Fourth Amendment: probable cause must exist; the officer who's seeking a warrant must support the warrant through an oath or affirmation; and the place, person, and thing to be seized must be clearly defined. Each and every one of these elements are supported by a plethora of case law.

Let's look at a few examples of the Fourth Amendment in action. In our first example, Dollree Mapp v. Ohio, is a very seminal case in Fourth Amendment law. The police received a tip that Dollree Mapp and her daughter were hiding a bombing suspect. They went to the Mapp residence and demanded entrance. Under advice of her attorney, Mapp refused to allow them into the residence without a warrant. That's an interesting point. The police show up at her house, and she has already consulted with her attorney. The police left and returned several hours later demanding to be let in. Mapp refused and the officers forced their way into the residence. Upon demand for the search warrant from the officers, they waved a piece of paper at her which they claimed to be a search warrant. She grabbed the piece of paper and shoved it into her blouse. One of the officers turned to her, reached into her blouse, and pulled out the piece of paper, after which the officers then handcuffed her.

Upon searching the house, the officers found a trunk in the basement that contained pornographic photos and objects. Mapp claims she was holding the trunk for a friend and wasn't aware of the contents. Mapp was arrested under Ohio law prohibiting the possession of pornographic material. At her trial, Mapp was convicted of the charge. The police did not produce a copy of the warrant when asked by the defense. So, the question is--was this a legal search? Well, obviously not.

Upon appeal to the Supreme Court, the Court stated that the exclusionary rule applies to the states as well as to the federal cases. This is why the case is so important, because now it extended the coverage of the Fourth Amendment from federal cases down to state cases. An exclusionary rule applies to states and evidence gained through illegal searches cannot be used. The court believed that the right to privacy as proclaimed in the Fourth Amendment is valid with regard to action by the states and so too should be the exclusionary rule.

Example 2, Ted Chimel v. the State of California. The police obtained a warrant to arrest Ted Chimel for the burglary of a coin shop. They went to his home, arrested him, and then, without a search warrant, proceeded to search the entire three-bedroom house including the attic, the garage, and a small workshop. During the search, the police found some of the stolen coins. Chimel objected to the search but agreed the police had the right to arrest him. He argued that if they wanted to search his entire house, then they should have gotten a search warrant. Was this a legal search?

A search without a warrant and incident to the arrest must be limited to the suspect and the immediate area around him. Thus, the search was illegal, and the statement by the court was that the police had plenty of time after the arrest to get a search warrant to search the entire house.

Example 3, Harold Garrison v State of Maryland. The Baltimore police officers obtained and executed a warrant to search the person of Laurence McWebb, and the premises known as 2036 Park Avenue, third-floor apartment. When the police applied for the warrant and when they conducted a search pursuant to the warrant, they reasonably believed there was only one apartment on the premises as described in the warrant. In fact, the third floor was divided into two apartments, one occupied by McWebb and one by Harold Garrison. You can imagine what happened next! Before the officers executing the warrant became aware that they were in a separate apartment occupied by Garrison, they discovered the contraband that provided the basis for Garrison's conviction for violating Maryland's Controlled Substances Act. They were in the wrong apartment,

but on the third floor. Garrison brought a Fourth Amendment claim that the police did not have a search warrant to search his apartment. The warrant had named McWebb, and so Garrison wanted to use the Fourth Amendment to suppress the evidence. Does Garrison have a case?

Well, no. The Supreme Court decided that since the warrant allowed for investigation of the third floor, the officers reasonably relied upon the warrant to carry out the search.

The fourth example, Carroll v. United States. George Carroll and two others were dealing in bootleg liquor in the Grand Rapids area. Federal agents attempted to set up a buy and fixed a price on the purchase. Carroll indicated he would have to go to the other side of Grand Rapids and would return shortly. For reasons unknown, he did not return. Later the Federal agents observed Carroll driving his vehicle from Detroit towards Grand Rapids on a road frequently used by smugglers. The agents stopped the vehicle and immediately searched the vehicle. Behind the upholstery on the rear seat, agents found 69 bottles labeled whiskey. The officers claimed that they had good reason to believe the car would contain illegal alcohol. Was this a legitimate warrantless search? Yes! A warrantless search of a car does not violate the Fourth Amendment. The mobility of the automobile makes it impractical to get a search warrant.

Unit 9, part 1

We've gone a few lessons without looking at electronic crime laws. Let's look at several others that are on the books and apply to some of the activities that we may see in the course of investigating activities in the company. We've already looked at the CFAA (the Computer Fraud and Abuse Act). We've looked at the Digital Millennium Copyright Act, and we looked at the Espionage Act. What I'd like to do in in this unit is look at the Electronic Communications Privacy Act (ECPA), The Pen/Trap Statute, Foreign Intelligence Surveillance Act, and the U.S. Patriot Act.

The Electronic Communication Privacy Act was enacted in 1986 and it extends government restrictions on wiretaps from telephone calls to transmissions of electronic data. We're looking at files and emails that are in a transient state. It also allows an ISP to look through all stored email and files under carefully established scenarios. It prevents those ISPs from revealing information in the files without the proper warrants and administrative subpoenas.

The investigators often need to obtain the destination, origin or even the contents of certain communications. Normally this information is considered private. So, you can imagine if there are activities taking place with your employees, such as downloading child pornography, law enforcement would be interested. They would be interested not only in that individual who's conducting that activity, but also from where that activity may have originated, and whether there may be other people who are collecting or distributing that particular type of data. The ECPA was designed to prevent misuse of computer information and protect all forms of electronic communications. It prevents unlawful access and unlawful interception of electronic communications.

To intercept electronic communications, law enforcement officers must follow very specific procedures and obtain a Court order that meets very rigid requirements. But the ECPA is more flexible with regards to accessing stored electronic communications than what we've had in the past. Law

enforcement officers can use administrative subpoenas (ordering a person to attend a court) authorized by federal state statute, and court orders or subpoenas that are issued by the Court. The distinction needs to be made between stored and intercepted communications, as intercepting communications is potentially a greater invasion of privacy. A stored communications example is email that's in your email box. If I intercept your email on the way TO your email box, then I'm intercepting a communication, and it's similar to an electronic wiretap. There are different rules that apply to communications that are on the wire. Stored communications are covered by the ECPA.

There's always a question of the expectation of privacy that people have with respect to their activities on a computer, or even in this case, the video rental places and books loaned from a library. You're expecting that if you rent a video that nobody is going to examine your rental history. If there are books loaned from the library, nobody's going to examine which books were loaned from the library. If you happen to do a search on Goggle, all bets are off. However, limitations do arise to that expectation. If a computer user has no reasonable expectation of privacy, a warrant is not required. This would be the case if a company issues an employee a company computer. Once I issue you a company computer, and I have made it a policy that you should have no expectation of privacy, then that lays out a different legal scenario than if you're using your own computer and I had no policy in place.

In the U.S. v. Simons, in the year 2000, Simons was a government employee working for the Foreign Broadcast Information Service or FBIS which is a division of the CIA. Simons was suspected of using the office computer to download pornography. Without a warrant, the CIA remotely accessed Simon's computer and over 1,000 pictures were found, some containing child pornography. Simons attempted to suppress that evidence claiming a violation of the Fourth Amendment and his expectation of privacy. The CIA has a very well-developed policy structure, and one of their policies, the Internet Policy, allowed for periodic auditing, inspection, and monitoring of the user's Internet access. The Court ruled that because an Acceptable Use Policy existed, and quite frankly because the CIA monitored and audited those internet access usages on a regular basis, that Simons had no reasonable expectation of privacy and thus no warrant was necessary.

In the U.S. v. Ziegler, the FBI was notified that an employee of the ISP provider for Frontline Processing and a fiancé of a Frontline employee was accessing child pornography. The FBI agent contacted the Frontline IT administrator, who verified that the employee Jeffrey Brian Ziegler was accessing child pornographic sites. Frontline was already monitoring Ziegler's traffic and Frontline owned and routinely monitored all workplace computers. There was some dispute in the case over who initiated the action of backing up Ziegler's hard drive, but a backup was made. There was at least one backup, but, in fact, I think several were made.

Frontline's corporate counsel indicated to the FBI agent that Frontline would cooperate with the investigation. They turned over Ziegler's computer to the FBI. The computer and one of the two backups of the drive were given to the FBI. The second backup copy was turned over sometime later. Forensics examiners found child pornography on the hard drive, but Ziegler sought to suppress the evidence obtained. His contention was that the FBI agent had violated his Fourth Amendment rights, and that a warrant was not sought, nor was one presented.

Ziegler contended that the FBI agent had directed the Frontline employees to enter his office and search his computer. The FBI agent countered that the search was voluntary and therefore was private in nature. The District Court held that the FBI agent did direct Frontline to make the backup copies of the hard drive. However, citing the Simons case, Ziegler had no reasonable expectation of privacy.

On appeal, Ziegler contended that entry into his private office to search his work computer violated the Fourth Amendment, and, as such, the evidence contained on the computer's hard drive must be suppressed. The Court reasoned since Ziegler was in a private office secured by a lock that he had a reasonable expectation of privacy, thus the Fourth

Amendment would apply. The Frontline employees conducting the search were considered by the Courts as de facto agents of the government by their actions. This is an important contention with the Fourth Amendment that I made by indirect reference in the Fourth Amendment section. The Fourth Amendment only applies to government agents…unless the government agents are in your corporate office and request you to provide them a backup, and you make the backup. You are now acting as a de facto agent of the government by your actions. The Fourth Amendment could apply by your activities. The remaining question was whether the search was unreasonable.

There's an exception to a reasonable search and seizure when there is voluntary compliance. But the question is who can give voluntary compliance in the workplace? Since the voluntary compliance was by Frontline, and not by Ziegler, the Court had to decide whether the company had possessed common authority or other sufficient relationship to the premises or effects sought to be inspected. The Court determined that Frontline could give consent to the search of the hard drive as the computer was workplace property and remained under the control of the company. Most importantly Frontline routinely monitored Internet traffic and employees were notified upon hiring that the company monitored the traffic. Thus, an expectation of privacy by Ziegler could not have been assumed.

The Court, thus, held that Ziegler had no reasonable expectation of privacy with respect to the use of his computer. In addition, the Court held that Frontline had the ability to give consent to a search of Ziegler's office and computer. Although Ziegler retained a legitimate expectation of privacy in his workplace office, Frontline retained the ability to consent to a search of Ziegler's office and his company owned computer. Because a valid third-party consent to search the office and the computer located there was given by his employer, the District Court's order denying suppression of the evidence of child pornography existing on Ziegler's computer was affirmed.

The interception of emails is prohibited by unauthorized individuals and individuals working for a government agency operating without a proper warrant. However, exceptions would be: if the individual gives you consent to intercept the email; if the provider of the communication service monitors communications; or if monitoring is done in the normal course of business. All three of those qualify as exceptions to those rules.

Individual consent can be implied, or it can be explicit. Some Courts have placed a high standard on what constitutes implied consent. It may not be enough to assume that there's general knowledge of monitoring taking place. In other words, it's not enough to assume there is common knowledge that the company does monitor. The employer needs to produce an Email Policy and an Acceptable Use Policy that clearly indicates that monitoring will take place. The employees should acknowledge in writing the context of the policy.

The provider of a communications service can monitor communications. Where this is an employer, the ECPA allows broad discretion to read and disclose the contents of email communication without the employees consent and monitoring is done in the normal course of business.

In companies that I've worked with, since we provided the computers and provided the email service, then we could examine the emails of individuals under the context of the HR and the legal departments. Should there be questions over some issue, this was perfectly legal under the ECPA. However, we also had an Acceptable Use Policy, Email Policy, and Security Policies which all had to be accepted in writing by the users, after reading and indicating they understood the policies.

Unit9, part 2

The Wiretap Act was passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. You may hear people refer to it as a wiretap or Title III Action, but wiretap was certainly an important aspect of fighting crime in the 50's and 60's. It's derived from the Supreme Court's ruling in Katz v. United States that the Fourth Amendment restricts the government's use of wiretap to eavesdrop on telephone calls. It contains a broad general prohibition on the intentional interception, procurement, and use of electronic, wire, or oral communications. It also prohibits the intentional interception of disclosure of the contents of unlawfully intercepted communications.

However, there are a number of exceptions to the Wiretap Act. For instance, if there is a telecommunications employee who needs to listen in on a wire for rendering service or protection of the rights of property of a provider, providers may provide information that the government is authorized by the FISA Court. Another exception is a law enforcement officer who's a party to the communication and is not subject to the Wiretap Act prohibitions. A third example is that a private individual may intercept a communication if that individual is a party to the communication, unless the interception is conducted in order to commit a criminal act. The Wiretap Statute prohibits electronic communications in transit, in general.

The Electronic Communication Privacy Act (ECPA) amended the Federal Wiretap Statute to include interception of electronic communications including email. The Federal Wiretap Statute states that immediately upon the execution of the period covered by the wiretap, a recording shall be made available to the judge issuing such order and sealed under his direction. The presence of the seal or satisfactory explanation for the absence thereof shall be a prerequisite for the use or disclosure of the contents of the intercept.

The ECPA may give you a pass on analyzing email that is static. Again, it's inside the mailbox. Email files that are in transit may violate a Wiretap Statute. The Cybersecurity Act of 2015 also can significantly enhance the ability for private entities to monitor systems and networks for cybersecurity threats.

Pen registers are devices or processes that record dialing, routing, addressing, or signaling information of wire and electronic communications. Now again, these were designed early on when telecommunication systems were analog devices and analog servers, but now they've been adapted to the digital world. The Pen Register Act restricts the collection of non-content communications data by the government and private parties. The U.S. Supreme Court has held that the Fourth Amendment does not restrict the government's use of pen registers to obtain non-content information. Non-content information are things such as logs of telephone numbers, metadata--things that do not contain the content of the conversation.

Trap-and-trace devices collect this metadata of incoming communications. The Pen Register Act does not apply to the contents of the communication. You can collect the metadata, but you cannot collect the content. A pen register requires a certification from a law enforcement officer that the information is relevant to an ongoing investigation. That is a fairly lenient bar to meet. All you have to do is to show that it's likely the information is likely to be obtained by such an installation, and you don't even have to show probable cause.

Section 3123 of Pen Register Act order must specify: the identity of the person to whom the telephone line or facility is leased; the identity of the person subject to the investigation; the attributes of the communication for which the order applies; and the statement of the offense to which the information is likely to be obtained by the device relates. That's all you have to provide to be able to collect that metadata.

The ECPA updates the Pen Trap Statute for non-content traffic: you can use the pen trap to trace communications over the internet and computer networks; any pen orders issued by a federal court has validity nationwide; and law enforcement must file a special report with the court.

An interesting concept is that of the National Security Letters. It's a controversial aspect of the 2001 USA Patriot Act. It was an extension of the government's ability to issue those letters. Their administrative subpoenas allow the government to secretly obtain certain information relevant to national security investigations and modified for privacy purposes. But the FBI can provide wire or electronics service providers with the name, phone number, and account number. These letters request the associated name, address, length of service, local and long-distance toll billing records. The service provider additionally cannot reveal the existence of these letters.

The Foreign Intelligence Surveillance Act (FISA) prescribes procedures for physical electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers. Interestingly enough, it's not just foreign agents but may include Americans and permanent residents suspected of engaging in espionage and violating U.S. law in the territory under the United States control.

FISA has multiple provisions such as electronic surveillance, physical searches, pen registers, trap and trace devices, access to certain business records, and reporting requirements. You can read through all of these in the indicated references.

Most importantly with the FISA is the concept of warrantless searches. The President of the United States may authorize the Attorney General to conduct an electronic surveillance for up to one year without a warrant. The Attorney General certifies to the FISA Court. It may also conduct warrantless searches for up to fifteen days at the start of a war. Warrant searches may apply for a warrant through the FISA Court if they want to execute searches that require warrants.

Unit 9, part 3

The U.S. Patriot Act has been one of the more controversial laws on the books. I love its full title here: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. if you look at the capital of each of those words, it's an acronym for USA PATRIOT Act. Like I said, it's a complex and confusing law that's been renewed several times. Its future is uncertain.

Title I, Enhancing Domestic Security Against Terrorism, establishes a Counterterrorism Fund, and, most importantly, prohibits Discrimination Against Arab and Muslim Americans, and establishes Presidential Authority. Now, there's a lot of provisions in the USA PATRIOT Act, and I'm not going to go through each of these. We'll highlight a couple, and, if you're interested, you can go through it and look at them in much more depth.

Enhanced Surveillance Procedures are under Title II. This refers to the authority to intercept wire, oral, and electronic communications relating to Terrorism and Fraud and Abuse Offenses. The ability to share criminal investigation information amends the Federal Rules of Criminal Procedures and allows Federal agencies to share information during investigations. The Duration of FISA Surveillance of Non-U.S. Persons Who are Agents of a Foreign Power amends FISA to allow 90-days of warrantless surveillance.

Title II also includes: seizure of voicemail messages; authority for delaying notice of the execution of a warrant (We'll talk about that shortly in this unit.); interception of computer trespasser communications; nationwide service of search warrants for electronic evidence. (This is an interesting provision.); and immunity for compliance with the FISA wiretap. Title II states : "No cause of action shall lie in any court against a provider of a wire or electronic communication service, landlord, custodian, or other person that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this act."

Title III, the International Money Laundering Abatement and Anti-terrorist Financing Act is an especially important aspect of fighting terrorism by fighting the funding of terrorism. Terrorists finance a lot of their operations through funding activities such as selling oil, drugs, and converting legitimate purchases or businesses into money laundering facilities. Money laundering is a particularly important aspect of the terrorist financing. So, Title III adjusts some of the rules and regulations around money laundering by tightening up that process. To give you an example: I worked for a payment company for a number of years. One of the things we had to monitor closely was potential money laundering opportunities. This would be where a criminal might set up a business and then funnel bad credit card information or stolen credit card information through a phony business for the purposes of converting that into cash.

Title IV - Protecting the Border; Protecting the Northern Border; Enhanced Immigration Provisions; and Preservation of Immigration Benefits for Victims of Terrorism.

Title V – Removing Obstacles to Investigating Terrorism includes using DNA identification of terrorists and other violent offenders. The use of DNA has become much more prevalent in the investigative world. There have been a number of criminals caught many years after their original crimes because DNA was collected for subsequent crimes committed. From what I understand, some of the DNA tests that you may take for genealogical research may in fact be shared with law enforcement. I don't have a citation on that one for you, so you may not want to take this literally. Disclosure of educational records is also in Title V. We'll talk shortly about the adjustments to FERPA (Family Educational Rights and Privacy Act)

Title VI - Providing for Victims of Terrorism, Public Safety Officers and Their Families. This provides aid to families of Public Safety officers and amendments to the victims of Crime Act of 1984.

Title VII - Increased Information Sharing for Critical Infrastructure Protection

Title VIII - Strengthening the Criminal Laws Against Terrorism. Interesting that in Section 802 is a definition of domestic terror. In fact, on slide 8, we have a definition for Domestic Terrorism as activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State and appear to be intended to intimidate or coerce a civil civilian population; acts that are intended to influence the policy of a government by intimidation or coercion; and acts to affect the conduct of a government by mass destruction, assassination, or kidnapping, and these occur primarily within the territorial jurisdiction of the United States. Fortunately, we don't have a great deal of domestic terrorism, but there are provisions for it, and certainly there are people inside government law enforcement agencies that are focused on identifying domestic terrorists.

Title VIII - Strengthening the Criminal Laws Against Terrorism. You can see this includes the definition of the federal crime of terrorism, deterrence, and prevention of cyberterrorism. A lot of effort has been focused on the cyber terrorism aspect of terrorism. It's not an unlikely scenario that in the future we may see terrorists operating in the electronic world as much as they operate in the physical world.

The Severability Clauses – You'll see this in contracts a lot. Basically, it says that if any provision inside the Patriot Act were found to be unenforceable or invalid, that would not affect any of the other clauses in the Patriot Act. It's a good way to protect the wholeness of the law or the Statute, in this case. Just as it would protect the contract you would have with somebody, if they try to break the contract by saying that one certain provision was unenforceable or invalid. In the case of a contract with a severability clause, that would not invalidate the contract nor would it invalidate the Patriot Act here.

The Patriot Act extended some of the statutes that were under other types of electronic crimes laws. The Federal Education Records and Privacy Act (FERPA) grew out of the anti-war protests for protection of students' records. They wanted transparency and access of the records limited to the individual student himself. FERPA recognized a shift from *in loco parentis.* This means that someone is acting as a parent for the student. Example, when you're off at college, even though your parents may be in the town, and on the college campus, the campus acts for your benefit and welfare and, therefore, is acting *in loco parentis*. There were already existing Health and Safety exceptions for individual students. The Patriot Act amended FERPA to permit the educational institutions to disclose educational same records to the federal law enforcement officials without student consent. There is a court order and the institution is not held liable. In the news, you may have seen occasionally an increase in activity of foreign agents acting as students in college universities. It's not unlikely for an investigation to revolve around a particular student whose activities may have drawn the attention of federal investigators

Federal Intelligence Surveillance Act (FISA) Amendments – When there is the FBI seizure with court orders of certain business records pursuant to an investigation of international terrorism, that record-keeper cannot disclose that FBI action to anybody, and the investigation is not to be conducted upon a U.S. person solely on the bases of activities protected by the First Amendment.

The Electronic Communications Privacy Act (ECPA) Amendments – This is amended with updates to revisions covering the telecommunication environment to include electronic information, such as voicemail which is now obtainable like email with a court order. It also covers the computer trespass where the owner/operator consents for federal investigation, and, when there's a reasonable belief the investigation is relevant to a computer trespass, no authorization is required, and no limits are established.

I think this is probably one of the neatest names for a provision: Sneak and Peek. The USA PATRIOT Act changes the point at which the target is notified of the search. Prior to the Patriot Act, if there was to be a search, you had to notify the target the search was taking place. Under the Act, the investigator can delay the notification for 90-days and can extend this delay even longer with a showing of good cause. This is limited to cases where there's a danger to life or safety of an individual; flight risk; witness or evidence tampering; or where immediate notification would jeopardize the investigation.

Unit 10, part 1

Privacy is one of the most important aspects of the job of a Chief Information Security Officer (CISO). We design our security strategies, compliance strategies, and risk strategies, but the issue of privacy interacts with all of these. It's essential that we are familiar with the privacy rules out there and know how to establish the privacy framework we want to operate within a company. For instance, do we have any responsibilities under HIPAA? Do we have any privacy policies? If so, do all interactions with our compliance or our clients comply with the terms of that privacy policy? How often do we review that policy to ensure it's up to date with respect to the various state and federal laws? Have we properly conveyed our privacy policy to our clients? Do we capture non-personal data in the course of working with our clients? As we continue through this unit, you will come to understand the significance of this question. "Do we have clients in California?"

Privacy limits a company's ability to collect, use, share, and retain personal information. The privacy laws define what we must do to protect the data that we collect. Such as: what are the legal restrictions on the use of that data? Can we sell non-public data to a third-party? Are there minimum safeguards we must have in place to protect the data from malicious actors? What happens if the data are misused? There's an intersection between our security and privacy practices that permeates our day-to-day operations.

As a refresher, the FTC under Section 5 declares illegal any unfair deceptive acts or practices in or affecting commerce. An unfair practice, as we saw in the first unit, was defined as a practice that is likely to cause substantial injury to consumers not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. As we saw with data security, the FTC hasn't defined any specific privacy rules.

And yet the FTC still expects companies to disclose material aspects of how they handle the data and to be honest in their statements about data processing. They premise some important principles: transparency; full disclosure; and honesty. But they do not specify the rules on data privacy.

However, like security, they have issued a pamphlet entitled Protecting Consumer Privacy in an Era of Rapid Change. It's not legally binding, but it does include five principles: privacy by design; simplified consumer choice; privacy notices; access; and consumer education. You will notice that privacy by design is parallel to another pamphlet they produce that talks about security by design. As you are designing an application, or service, or collecting data you want to make sure you incorporate the aspects of privacy. Unquestionably, access control is a crucial! You must be aware of what level access to data that individuals will have and what rights do consumers have with respect to the data that you collect?

In 2013, the FTC issued another report with best practices for mobile applications. This report set up recommendations for application platforms and developers. You can see best practices in the guidelines: just-in-time disclosures and opt-in consent, particularly when you're collecting things like geolocation data; one-stop dashboards for customers to review content accessed by the apps they have developed; privacy best practices so developers can make privacy disclosures; review of the apps for privacy practices before they're made available to public; and implementing a "Do-Not-Track" mechanism.

The FTC recommended that you: post a privacy policy that is easily accessible; to use just-in-time disclosures and opt-in consent for collecting and sharing sensitive data; to coordinate with the ad networks and other third-parties to provide accurate disclosures to consumers; to set up self-regulatory programs to provide guidance on uniform, short-form privacy notices. These short-form privacy notices are much easier for consumers to read than are the ones that are just packed with legalese. The FTC continually looks at how technology changes can affect privacy, particularly in topics of geolocation and biometrics. We see this in many cases today.

The White House Consumer Privacy Bill of Rights was put out in 2012 by the White House. It’s non-binding and shows flexible and clear practices that apply to personal data, including aggregations of data and data that's linkable to a specific individual.

There are certain topics that they included in the Consumer Privacy Bill of Rights such as: individual control; transparency; respect for context, which means the data that you collect will be used and disclosed within the context in which you provided the data; security – consumers have a right to secure and responsible handling of personal data; access and accuracy-ensuring consumers have a right to access and correct personal data that might be collected; focused collection-meaning you're collecting the minimum amount of data necessary; and accountability-that the consumers have the right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

Unit 10, part 2

Let's look at how privacy applies to certain regulations that we've already looked at, for instance, HIPAA. Privacy is very restrictive in the healthcare industry. We looked at the security rule earlier in the course, but HIPAA also has implemented a Privacy Rule. It limits the use and disclosure of protected health information which relates to an individual's physical or mental health or condition to health plans, health care providers, health care clearing houses, and business associates. These are called covered entities. It only applies if the information identifies the individual and does not apply to de-identified information. That's important in research where information may be aggregated at a hospital or by a healthcare provider, and then included in a Health Study.

The Privacy Rule allows covered entities: to use and disclose protected health information to the individual for treatment, payment, or healthcare, incidental to the permitted use or disclosure; to place it in a facility directory; or to notify friends and family of care. If the use or disclosure is in the public interest and as required by law, the covered entities may also use and disclose it: for public health activities, regarding victims of abuse, neglect, or domestic violence; for health oversight activities; for law enforcement purposes; or for workers' compensation.

If not covered explicitly by an exemption, the covered entity or business associate is required to obtain the individual written authorization specifically allowing use and in allowing disclosure. I assume that the healthcare provider is reviewing the privacy rules and regulations on a

regular basis and updating their privacy notices appropriately. They should make reasonable effort to use or disclose the minimum necessary information. Minimum doesn't apply if the records are needed for treatment, disclosed to the individual, or disclosed under an authorization by the individual.

However, every health care provider must designate a privacy officer. One of the jobs of the privacy officer is to train all employees on how to maintain privacy of HIPAA records. In addition, you need to implement all the data security requirements that were under the HIPAA security rules. It requires entities: to provide consumers with "adequate notice of the uses and disclosures of protected health information" made by the covered entity to protect the individuals' rights; to know their legal duties with respect to protected health information; and to get a written acknowledgement from the individual.

Gramm-Leach-Bliley Act (GLBA)--within this act there are certain privacy rules that also are applied. Non-public financial data receives special protection, and where we looked at the security rules earlier, GLBA also has privacy requirements which they call the Privacy Rule. It's less burdensome than the HIPAA requirements, but it does require two things-- notice and choice.

Notice is simply providing privacy notices at the time the relationship with an individual commences and once a year thereafter. The notices must provide clear and conspicuous disclosure of a company's privacy practices

and disclosure of any non-personal data to third-parties; the categories of persons to whom data may be disclosed; and the company's security policies.

Choice allows users to choose whether to permit certain types of information sharing with non-affiliated third-parties, such as those who are performing services for the institution or other purposes. Choice also takes effect in notifying the individual of intended sharing, and the individual then has the right to decide whether or not that sharing should take place.

The California Financial Information Privacy Act imposes stricter privacy requirements on financial institutions. The California FIPA is codified to show that companies must receive opt-in consent from consumers prior to sharing their data with unaffiliated third-parties. It requires companies to allow consumers to opt-in, whereas with GLBA, companies are allowed to give customers the capability to opt-out. Opt-in, as you can imagine, requires explicit consent because you have to check the box or signify with a “yes” that you are allowing that opt-in capability. This restricts a financial institution’s ability to share personal data with affiliated companies. So, again, the customer must specifically provide an opt-out consent, in that particular case.

The CAN-SPAM Act is fighting the increase of the amount of junk mail, particularly spam messages. I don't know if you comprehend how many spam messages hit a company on a regular basis. In a company that I worked for recently, the number of spam messages literally were millions of messages a week. Fortunately, we had mechanisms to filter out spam messages so that very few got through to the employees. That doesn't

mean the attackers still aren't trying to get that information in to us. When you see the statistics, it is quite an amazing number. Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) in 2003. It is enforced by the FTC and the Federal Communications Commission (FCC). It's criticized in some corners because it preempts state laws and prevents consumers from bringing private actions against spammers.

There's a prohibition against false or misleading transmission of information. This prevent senders of commercial email from sending false header information, such as email addresses and IP addresses. I'll show you an example shortly. The email must accurately reflect the identity of a protected computer used to initiate the message. The email headers can be a clue to the veracity of an email message, particularly since the CAN-SPAM Act has a provision prohibiting deceptive subject headings, return address or opt- outs, and identification of an email advertisement.

I have a couple of examples on slides 10 & 11. On slide 10, the examples are valid emails that came to me. Actually, I believe these are both the same message, so let’s refer to this as one message. It's a valid message and a valid advertisement campaign. In fact, I believe you can see here, Precedence: bulk. It's from a company called Levenger. You can see here the email address that was generated by where it was from, and the line: “Subject: Summer Sale Finds Under $100”. It also has a very specific email address associated with it, and it has a “Reply To”. It is clear that it's going to Levenger and is going to the campaign they put together. You can

see the return path, reply to, and the message are all similar and pointing to the same thing.

On Slide 11, let's look at the email message I found recently in my junk folder. This clearly is not a legitimate message. What do you notice that identifies this as spam? The first thing that strikes you is that there is no Subject. More importantly, look at some of the anomalies, the "Reply To" is Stella Morris0600gmail.com and the email lists the origination address as Zenithcompensationhouse@gmail.com. If I remember correctly, this was some sort of a "get some money" scheme. But you can tell in this case this is not a legitimate email that was sent out to me.

Unit 10, part 3

The Video Privacy Protection Act (VPPA) was passed in 1988 to protect the privacy of video cassette rental information. Though this technology is outdated, the law continues to have a big impact on website and application development. It basically prevents a rental company from disclosing an individual's personally identifiable video requests, viewing habits, without informed written consent of the user. I think this stemmed from the hearings on Judge Bork when he was up for nomination for the Supreme Court. It was some of his video rental information that may have been leaked at that point in time.

The law basically defines a video tape service provider as any person engaged in the business in or anyone affecting interstate or foreign commerce of rental sale or delivery of pre-recorded video cassette tapes or similar audio-visual material. So, you think to yourself, oh,wow! How does this apply today? This is old technology, and in fact it is difficult to find VHS recorders and tapes. But the definition is very broadly interpreted by the Courts. Think about what it's protecting. It’s protecting rental information regarding content that a user is either viewing or reading. In the 2012 case in Federal Court, it was ruled that Hulu's online movie streaming service is covered by the VPPA. The consent must be separate and distinct from any other legal or financial notice, either through a pop-up, or with an affirmative act such as clicking on a button to agree.

The Children's Online Privacy Protection Act (COPPA) restricts the online collection of information from minors who are under the age of 13 years. The FTC enforces this law, and it applies to the two types of website and online services. Those types that are directed at children under the age of 13, and those types that have actual knowledge that they are collecting or maintaining information from children under the age of 13. To differentiate whether a site is directed at children under 13, the courts will look at things like: subject matter; visual content; animated characters; children-oriented activities; the age of the models; use of celebrities that appeal to children; language or other characteristics of the service; and whether advertising on the site is directed at children.

If covered under COPPA the websites and the online services must provide clear notice on the site that they collect information from children, how they use that information, and the disclosure practices for the collected information. The website must obtain verifiable parental information before collecting, using, or disclosing any personal information from children under the age of 13. The type of information they might collect is: first and last name; physical mailing address; online contact information; telephone numbers; social security numbers; geolocation information; screen or usernames that function as contact info; persistent identifiers that can be recognized as the user; photographs, videos, or audio files containing the child's image; and information on the child or parents collected with any of these identifiers.

Verifiable parental information that you might use as consent are: signing a consent form and returning it by postal mail, fax, or electronic scan; use of a credit card or debit card or other payment mechanism that notifies the holder of the activity; phone call from a parent; parent connection to a company through a videoconference link; other forms of government-issued identification such as a driver's license, passport, etc.; and, in some cases, you can use Email if the collected information is only for internal operations and not passed on to a third-party. This can be done using SMS messaging or a delayed second email message.

Unit 10, part 4

We'll finish up this unit by looking at some of California's online privacy laws. As I said, we look particularly at California for various reasons. Each year we need to adjust our policies and practices, and it's a common practice for CISOs to use the strictest available guidelines as a baseline for their practices. That way, if you meet the strictest requirements, then all other states will be in line with your privacy requirements. You continuously review the state and federal policies for changes. California leads the nation in some of the strictest, most comprehensive online privacy laws. Importantly, the California laws tend to address issues facing the internet world, and that's why I think California leads the pack in trying to understand and set forth privacy regulations that protect an individual's privacy on the Internet. The California privacy laws often present a challenge, though, to corporate security teams. Because of their restrictiveness, it sometimes puts the onus on the companies to find new ways of handling data, or collecting data, or presenting interfaces to the clients that can be very costly to implement

California Online Privacy Protection Act (CalOPPA) was instituted around 2004. In that timeframe there really wasn't a need or a requirement to post a privacy policy. It was generally accepted that, if you did post a privacy policy, it had to reflect the actual practices that were in place. Well, CalOPPA required all companies that collected personally identifiable information to conspicuously post a privacy policy. This required a company to address two issues: designing a privacy policy and designing and implementing the actual practices behind the policy. I don't know if it's a chicken and an egg kind of thing. Do you design the privacy policy, and then institute the actual practices behind that to ensure they match up? Or do you match up the privacy policy with the practices that you have in place? It's probably both. Those practices which don't match other aspects of California law or Massachusetts law, or whatever, you'll certainly want to have updated before you write your policy, and then your policy would reflect your actual situation.

CalOPPA set certain minimum privacy policy elements, such as:

categories of personally identifiable information collected; categories of third-parties with whom data might be shared; descriptions of any processes that consumers can use to review and request changes to information; descriptions of the process that will notify all users of material changes; and establishing effective dates of the privacy policies. An important aspect of effective dates of privacy policies are that as privacy policies change, or as regulations regarding privacy policies change, you still need to keep track of old privacy policies. If a lawsuit is filed against you for an activity that took place in the past, you will want to know what privacy policies and security policies applied to the organization at that period of time. You want to make sure you keep track of the information in those policies; a description of "Do Not Track" requests and how that will be handled will also need to be maintained.

Personally identifiable information of an individual includes: first and last name; home address or other physical address; email address; phone number; social security number; or other identifier that permits physical or online contact of an individual; or any combinations of these elements. There are variations in California statutes that go further to define the elements of personally identifiable information. You don't want to just rely on one law; you want to look at the entire mix of California laws. The California Attorney General aggressively enforces this policy and today CalOPPA requires mobile apps to post a privacy policy as well.

The California Shine the Light Law went into effect in 2005. It applies to companies that have established business relationships with customers. It applies to companies that have disclosed personal information during the past calendar year to third-parties for direct marketing. I'm not going to read through the categories of personally identifiable information, but you can see this is a fairly lengthy list of information. Some of the interesting ones are in the middle of the second column, such as political party affiliation, kind of product purchased, your kind of services performed, age and gender of children, etc. These things definitely are personal information and certainly could lead to being personally identifiable information.

Upon request by the customer, the company must supply whatever information is stored on the customer for free. Company must provide contact information, either an email address or mailing address, should the customer need to contact company. Companies receiving a Shine the Light request must respond within 30-days.

The California Minor Eraser Law is an interesting law that went into effect in 2015. It places restrictions on websites, and online services and apps directed towards minors. However, it sets the age limit for minors as being under the age of 18, not 13. It provides minors a limited ability to request and obtain removal of content information that the minor may have posted on the site. The site must provide the minors with instructions on removing data, but there are some limitations on the ability to do this.

Another law that's fascinating is the Illinois Biometric Information Policy Act. It's used to limit the use of facial recognition and other biometrics. It defines biometric identifiers as a retina or iris scan, fingerprint, voiceprint, scan of a hand, or face geometry. It specifically excludes photography, writing samples, and physical description of the individuals. Biometric information on the other hand, is information regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. What's interesting in these biometric laws is that you don't see DNA listed. I'm wondering how long it will be before we start to see the biometric identifiers include the DNA that genealogical sites collect and hold in their databases.

The statute was key to a May 2016 case where a federal judge refused to dismiss a class action lawsuit against Facebook. The plaintiffs claimed that Facebook violated the Illinois law with its Tag Suggestions program. Basically, what Facebook did is to go out to photos that individuals put out on the internet and in Facebook, scanned the photos, and used facial recognition software to suggest “tags” to users to assign names to photos. Facebook claimed that the photographs were excluded from the law, but the Court disagreed and denied motion to dismiss. The Court reasoned that

the facial recognition technology constituted a “scan of face geometry” which is covered by the statute. Consider what Facebook was doing. In your Facebook account you store pictures of yourself and your family, which you might have tagged or you might have just noted somewhere in ilcapturing these images, scanning these images, and performing facial geometry and recognition on the faces in the pictures. Then they were matching those up with identified names in accounts and suggesting in other pictures on Facebook accounts that picture might be you by tagging it as you. Anyway, Illinois companies must get consent before using digitized images.

Unit 11, part 1

We begin Unit 11 looking at International Data Privacy. Up until now, we have focused on the laws governing data security, privacy, and compliance in the United States. In the United States, as we've seen, the privacy framework is a patchwork of state and federal laws and case decisions that are essentially varied by jurisdiction. The European laws and those of many countries have taken a more central approach to defining their privacy laws by their government bodies. In this unit we will address how some of these countries, the European Union (EU), Canada, China, Mexico, and Japan address privacy.

Two concepts that are similar across many countries are the concepts of a data controller and a data processor. The data controllers help determine precisely how data are used, distributed, shared, collected, and processed. While the data processors process data under the direction of the data controller.

The EU comprises 28 member nations, 19 of which have adopted the Euro, and is subject to the decision on Brexit. In 2016, the EU replaced its existing privacy legislation the Directive 95/46/EC with the General Data Protection Regulation (GDPR). The implementation date of the GDPR was May 25, 2018, so the GDPR is the "law of the land" at this point. The most fundamental statement on privacy in the EU is that it views privacy as a human right. The GDPR applies to the "personal data" processing of EU residents whether the processing takes place within the EU, or anywhere else in the world.

Personal data is any information relating to an identified or identifiable natural person. A natural person can be one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier, or one or more other factors such as physical, physiological, genetic, mental, economic, cultural or social identity. It does not have to include the individual's name, just identifiability.

The GDPR applies to two types of companies, the controllers and the processors. Controllers have the responsibility to ensure that processors are implementing the appropriate technical and organizational measures that meet the GDPR requirements. It's important to understand whether your company is a controller or a processor. For instance, a large retailer may be a controller since they collect data on users and employees. Their third-party payroll, HR, and credit card processors may in fact be classified as processors under GDPR.

The general principles of GDPR: are lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality. The processing of personal data is lawful only if: the individual has provided consent to the processing of personal data; the individual is subject to a contract for which processing is necessary; processing is necessary to protect "the vital interest of the data subject"; processing is necessary to perform a task in the public interest; or processing is necessary for the legitimate interest of the data controller or the third-party.

Additional restrictions on the processing of "special categories" of sensitive data which reveal: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; processing of genetic data; biometric data; health data; and sexual orientation. You'll notice they have included processing of genetic data which I posed as a question in the last unit about the biometric data being collected and being referenced in the Illinois Biometric Law. The individual must give explicit consent to conduct the processing.

The processing must be transparent, and it must provide the data subject with a number of different pieces of information such as: contact information for the data controller and data protection officer; purposes for the processing, and the interests of the controller or the third-party; recipients or categories of recipients of the personal data; whether the data

controller will transfer data to another jurisdiction; the length of time the personal data will be stored; the right to request access to and erasure of the data; the right to withdraw consent; the right to complain to a supervisory authority about whether the data are required by statute or contract; and the existence of automated decision-making such as profiling.

Additionally, in Article 17, the EU expresses the “right to be forgotten”. This is a qualified right to request data controllers to erase personal data if one of these conditions exists: the personal data is no longer necessary to serve the purposes for which it was collected or processed; the data subject has withdrawn the consent that allowed the personal data to be collected; the data subject objects and the controller fails to demonstrate compelling legitimate grounds for the processing; personal data was processed unlawfully; the EU or member state requires erasure under a different law; or personal data was collected from a child under 16. The controller is not required to delete the data if it is necessary for processing.

The GDPR does not prescribe specific data security provisions. It reads “...must “implement the appropriate technical and organizational measures to ensure a level of security appropriate to the risk”. However, suggestions for some technical measures are encryption and pseudonymization of the personal data. That can mean obfuscating certain fields like we do with credit card data, or it could be using hashing to protect the data encryption. Safeguarding the ongoing confidentiality, integrity, availability, and resilience of processing systems and services is another suggestion and a key technical approach, as well as, regular testing of technical and organizational security measures.

For data breach notification, the controller must, without undue delay and if feasible within 72 hours, notify government regulators and provide the following information: the nature of the breach; categories and number of data subjects; categories and number of personal data records involved; the name and contact details of the controller's data protection officer; the likely consequence of the data breach; and measures already taken to mitigate the adverse effects of the breach. However, there's no real

specified time limit to notify the data subjects of the breach. Notifications to individuals should have the same information as is sent to the regulators.

Exceptions to the "need to notify individuals" are: when the data was encrypted or anonymized; when the high-risk to the data subjects has not materialized. When individual notices would involve disproportionate effort, the controller can provide notification by public communications. Of particular concern to U.S. companies is a restriction on transferring covered data to a third country. Data must be deemed by the European Commission to have adequate protection for personal data. There are only 10 companies that have been deemed to have adequate protection.

Safe Harbor was a self-certification that companies have compiled with specific data protection principles, but this was struck down in 2015. It was replaced with the Privacy Shield in 2016 with the following provisions: notice; data integrity and purpose limitation; choice; data minimization; security; access; recourse, enforcement, and liability; and accountability for onward transfer.

Unit 11, part 2

The Canadian Privacy Law is called Personal Information Protections and Electronic Documents Act (PIPEDA). Like other countries, Canada established it at the national level as opposed to the U.S. approach. There are basically ten principles espoused in PIPEDA.

The first principle is accountability. This means simply: designating a privacy and security officer; providing those identities upon request; contractually requiring the third-party providers to protect personal information; establishing procedures to protect personal information; and training the staff on the protection of personal information.

Identifying purposes: identify the purposes that personal information is collected for and before the collection is made. Communication can be provided orally or in writing, and consent is required if personal data is to be applied for a different use.

Consent: must be obtained before collecting, using, or disclosing personal information. Consent can be obtained in different ways, but there are limited exceptions to the consent requirement.

Limiting collection: must limit personal information to that which is necessary, and usually Canada uses volume and type to determine how much personal information can be collected.

Limiting use, disclosure, and retention: information can be disclosed and used only for the stated purpose and the data must be disposed of once it’s no longer necessary.

Accuracy: companies must ensure that the data they hold is updated, complete, and accurate.

Safeguards: these are to be directed towards data security. These safeguards must be appropriate to the sensitivity of the data that's being collected. There’re basically three types of safeguards that can be implemented: physical measures; organizational measures; or technical measures.

If you look at some of these safeguards, they can be: risk management principles and practices; security policies; human resources security; physical security; technical security; incident management; and business continuity planning. If you basically use either the NIST Cybersecurity Framework or ISO 27001/2700 - or the NIST SP 800-53 and apply the principles of those frameworks, you'll be more than covered for the safeguards that they're looking for. It's just simply a matter of understanding those frameworks and applying the principles that they propose.

Openness: being open tells individuals: how the companies handle their data; and provide guidelines on how to contact the company and access their data. You can do this through handouts, brochures, and other documentation.

The ten principles continued:

Individual access: individuals have the right to contest accuracy and completeness of the information. The only exceptions are if it's too costly to provide, if there are legal restrictions on the disclosure, and the information contains information about other people.

Challenging compliance: individuals have the right to challenge a company's compliance. In the U.S., these challenges can only be made by government agencies; but, in Canada, companies are required to address all complaints and take appropriate measures.

A 2015 Amendment to PIPEDA added data breach notifications: if a company determines that a data breach creates risk of significant harm to the individual, it must file a report with the Privacy Commissioner and must notify the individual. The company must consider the sensitivity of the breach data and the probability that the data is being, or will be, misused; and other factors prescribed by law. The breach notices must contain enough information that the individual understands the breach and how to take steps to reduce the harm. Currently there are three provinces not covered under PIPEDA. I believe they are Alberta, British Columbia, and Quebec.

Unit 11, part 3

In this section we'll look at the laws of Mexico. There is the Mexican Federal Law on the Protection of Personal Data Possessed by Private Persons. While similar to the EU provisions, the key difference is that Mexico does not restrict export of personal information to countries without adequate data protection. Additionally, the data controllers have greater responsibilities in Mexico. The law broadly applies to all companies' privacy, processing, and handling of Mexican residents' personal data, either any identified or identifiable individual.

Some of the principles of the law follow:

Legality and Legitimacy: Controllers may not violate any legal restrictions on collection or processing of personal data.

Consent: must be given before the personal data is collected. Consent may be inferred if the individual receives a notice and doesn't respond, but, otherwise, expressed consent is required. It can be verbally, in writing, electronically, or by some unmistakable indication. The users may revoke consent at any point in time.

Notice and Information: controllers must provide a privacy notice describing what information is being collected and why. There is certain prescribed information that must be on those notices.

Quality: the controller is responsible for ensuring the personal data is correct, up-to-date, and relevant. And, once no longer needed, it must be deleted.

Purpose: the data can only be processed for the intended purpose.

Fidelity: it presumes a reasonable expectation of privacy. The law prohibits obtaining information deceptively or fraudulently.

Proportionality: data may be processed as necessary, appropriate, and relevant. You must make reasonable efforts to limit the processing period.

Accountability: data controllers are responsible for ensuring compliance with Mexico's privacy laws.

In addition to privacy the data controllers must implement physical, technical, and administrative data security measures. But the law doesn’t specify what those data safeguards are. You must consider the following factors: the inherent risk for the type of data that's being collected; the sensitivity of that data; the technological development; and potential consequences for individuals if security is violated. You should understand the number of data subjects, the risk factors, and previous vulnerabilities that have faced the company. Again, if you use a data security framework such as the NIST Cybersecurity Framework ISO 27001/2700, or NIST 800-53, you should be adequate in those security safeguards.

The regulations in Mexico do indicate what the controller should do at a minimum. That is: to inventory all processing systems and personal data; to determine the duties of personal data processors; to conduct a risk analysis; to establish, implement, and audit security measures for personal data; to conduct a gap analysis to determine missing security measures; to develop a plan to fill those gaps; to conduct security reviews (vulnerability analysis and penetration testing); to provide security training for all employees who process personal data; and to maintain records of personal data storage media. Controllers must document all these security measures.

In the case of a breach, the controller must conduct an exhaustive analysis of the breach. If the breach significantly impacts the data subject’s property or rights, the controller is required to notify the data subject without delay. Notice must include: a description of the breach; an inventory of the types of personal data potentially compromised; the recommendations for how the data subject may protect his own interests; corrective actions the controller has put into place; and instructions to obtain more information on the breach. The controller must conduct a thorough analysis of what caused that breach.

Unit 11, part 4

In this last part of the Unit, I'd like to look at China and Japan. In China some data security and privacy laws have been enacted, but it's difficult to judge how aggressively these will be enforced. China does not have government regulators focused on enforcing these laws. In 2012, the Standing Committee, the National People's Congress, issued the Decision on Strengthening Network Information Protection, which imposed new privacy obligations on some companies. But, it's unclear how broadly the law was meant to be enforced. Internet service providers and others that collect personal data were included under this particular law. Companies must abide by principles of legality, legitimacy, and necessity.

A 2015, report - European privacy experts criticized the scope of the Chinese privacy laws: the focus was internet only; there was no enforcement mechanism; there were no basic data subject rights; and principle setting was not as complete as the EU model. In 2013, there had been amendments to the Chinese law which reiterated that companies will abide by the principles of legality, propriety, and necessity. They must explicitly state why the means and scope of data are being collected and obtain consent from the data subject. They must keep collected data confidential and must not disclose, sell, or illegally provide that data to others. They need to implement technical measures to protect consumers' personal information from being disclosed or lost. They must immediately adopt remedial actions if personal data are lost or disclosed. They must not send commercial information to customers without their consent. Still, there's some concern over how aggressively these laws will be enforced.

In 2013, the Ministry of Industry and Information Technology provided more detail on security and privacy in a law called Information Security Industry Guidelines for Personal Information Protection on Public and Commercial Service Information Systems. It outlined how personal data will be managed, and its computer data handled in computer systems, as it relates to a specific natural person which can be independently, or in combination with other data information, identified.

This Chinese law laid out Eight Principles:

1. Clear purpose;
2. Least sufficient use;
3. Open notification;
4. Individual consent;
5. Quality guarantee
6. Security guarantee
7. Honest implementation
8. Clear responsibilities

In Japan, privacy stems largely from the 2003 Act on the Protection of Personal Information (APPI). It's similar to the comprehensive EU approach on data regulation. However, it's more stringent than the U.S. sectoral approach. Different from the EU, Japan law: does not require additional restrictions on sensitive data; does not differentiate between data controllers and data processors; does not require other countries' laws to be adequate before allowing foreign data transfers; and the definition of personal data is very broad and suggests that personal data protection is a human right.

The key duties imposed upon businesses that handle Japanese residents' data are: the utilization of the data must specify the purpose--you cannot unreasonably change the scope of the purpose; you must obtain prior consent before collecting the data; you must practice proper acquisition without using deception to acquire personal information; you must give notice at the time of data acquisition; and you must notify the user of the purpose of the data. These do not apply if it's necessary to comply with law enforcement.

Accuracy is also imposed: you must endeavor to maintain accurate and up-to-date personal data.

Security controls must be in place: the business operators need to take necessary and proper measures to protect data and to prevent leakage, loss, or damage. It does not specify what those particular safeguards need to be. Again, you could use a framework to guide you in that process.

Employee supervision is needed that ensures that employees handle data properly.

Transfers to third-parties: You may not provide personal data to third-parties without prior consent. The only exceptions are if the transfer is based on laws or regulations or if the transfers are necessary to protect individuals or property and the consent would be difficult to obtain. It makes public health data or child welfare and consent difficult to obtain; it is necessary for all to cooperate with the government.

Public privacy notice: companies must post a publicly accessible document containing the name of the business officer responsible for handling personal information; the purpose of the data to be collected; and procedures for handling requests for personal information from the data subjects.

Business operators must generally correct, add, or delete personal information at the request of the data subject.

In 2017, Japan implemented a Privacy Protection Commission to enforce Japan's privacy laws.

China

- Eight principles
  - Clear purpose
    - Specific, clear, and reasonable purpose to handle personal data
    - May not alter purpose without notifying the data subject
  - Least sufficient use
    - Use least amount of data
    - Delete data when no longer needed
  - Open notification
    - Properly notify data subjects
    - Clear, easily understandable, and appropriate ways
  - Individual consent
    - Obtain consent from data subjects before collecting data

China

- Eight principles (con't)
  - Quality guarantee
    - Must guarantee that data will be secure, intact, and usable
  - Security guarantee
    - Implement sufficient administrative and technical safeguards
    - Protecting personal information security
    - Preventing retrieval or disclosure of the information without authorization
    - Prevent loss, leakage, destruction, and alteration or personal information
  - Honest implementation
    - Abide by promises made
  - Clear responsibilities
    - Clarify responsibilities for handling personal information so it can be traced

Unit 12, part 1

Since 2013 with the leak of highly sensitive information and documents from the NSA by Edward Snowden, the U.S. government has looked more closely at the cybersecurity practices of the contractors that are working for them.

The level of cybersecurity requirements for a federal contractor increases as the sensitivity of data and information increases. All contractors must abide by the provisions of the Federal Information Security Management Act and NIST Special Publication 800-53, of which I've mentioned several times when we talked about security frameworks. Contractors that handle classified information have more stringent regulations enumerated in the National Industrial Security Program Operating Manual (NISPOM). A newly unclassified category has been created for information that's not classified but is sensitive. It's called Controlled Unclassified Information (CUI).

The Federal Information Security Management Act (FISMA) is a framework for information security. It was updated with the Federal Information Security Modernization Act in 2014. The scope of the FISMA covers both government agencies as well as federal contractors. Thus, if you are a federal contractor or work for a company that has federal contracts, you will have to be compliant with FISMA. The FISMA delegates part of the information security program to the Office of Management and Budget, such as the development of government-wide information security policy standards and guidelines and the coordination with NIST on standards and guidelines.

FISMA has several requirements: implementing information security practice protections commensurate with the risk and magnitude of harm; undergoing information security risk assessment from senior agency officials; implementing necessary protections, and testing and evaluating the information security controls; delegating the formation of security compliance to a chief information officer; overseeing agency information; security training; reporting annually on the effectiveness of agency

information security controls; and holding personnel accountable for complying with the program.

FISMA is a comprehensive program. It encompasses: periodic risk assessments; policies and procedures based on the risk assessments; subordinate plans for information security; security training; annual testing and evaluation of policies and procedures; remedial action to correct security flaws; security incident detection, reporting, and response procedures; and continuity of operations.

FISMA has regulations on breach notification. You have to report expeditiously, and there needs to be: a general description of the breach; an estimate of the number of individuals whose information was disclosed; a description of circumstances which delays notification; and an estimate of when the agency will notify individuals. I have a reference here, over to the right, of, certainly, one of the most devastating attacks in government databases by the OPM hack. Certainly, if you're interested, you could follow that link to get more information.

Unit 12, part 2

FISMA delegates responsibility for information security standards to the National Institute of Standards and Technology (NIST). The NIST website maintains a repository of many standards for information security. If you can go to "htpps://csrc.nist.gov", you'll find a plethora of documents about securing your system. Some will be very technical and some less technical, but certainly there are documents there that cover the spectrum of information security. The documents are basically in three different categories:

Drafts - which are documents and standards which have not been published, may still be in development, or just out for comment--just not yet published.

FIPS - the location of the FIPS 199 and 200 documents which you use to start building your minimum-security controls.

Special Publication (SP) 800's – the location of SP 800-53, which we're going to look at here. It coordinates with a menu of 17-controls from FIPS 200. It's based on low, medium, and high risk.

The first of the SP 800-53 controls is:

Access Control: you must ensure that only authorized users, processes, and devices are permitted to access the information system. You can see listed here the large number of controls from account management: lease privilege; concurrent session control; remote access control; wireless access; data mining protection, etc.

Awareness and training: you must ensure that managers and personnel are adequately trained on information security. This includes: training on your security awareness and training policies and procedures; role-based security training. You must maintain those security training records and the contacts with security groups and associations.

Audits and accountability: audit records should be enabled to view monitoring, analysis, investigation, and reporting of unauthorized activity. They should be traceable to individual users. You can see here the list of audit and accountability procedures from audit events: the audit storage requirements; time stamps; audit review analysis; protection of audit information; and non-repudiation.

Certification, accreditation, and security assessments: this requires periodic assessments of security controls to determine if current systems are effectively controlled. This is managed through security assessments, security interconnections, system certification, continuous monitoring, and penetration testing.

Configuration management: you must establish and maintain baseline inventories and configurations of hardware, software, firmware, and other information systems. This includes: baseline configuration; configurations change control; security impact analysis; lease functionality; information system component inventory; software usage restrictions; and user installed software practices.

Contingency planning: You're required to develop plans for operating your information systems during emergencies to ensure continuity operations. This is where you would have: your continuity plans; contingency training;

contingency plan training; alternative storage sites; and information system backups.

Identification and authentication: you must accurately identify authorized users. You have listed here: your practices towards identification and authorization of users; device identification and authentication; identifier management; and service identification and authorization.

Incident response: you must develop comprehensive plans to detect, contain, and respond to incidents and to report such to authorities. This includes: incident response training; incident response testing; incident handling; incident monitoring; incident reporting; and your incident response plan.

Maintenance – you must regularly maintain information systems and security controls. This has standards for your maintenance tools, maintenance personnel, and timely maintenance itself.

Media protection: you must limit access to system media to authorized users and permanently wipe media before disposal. The controls that are listed here are media access, storage, sanitization, use, and downgrading.

Physical and environmental protection: you must restrict physical access to authorized individuals only and protect the systems from environmental hazards. These are all the things you would think of in terms of physically securing your systems: physical access; monitoring physical access; visitor

access records; emergency power; fire protection; temperature and humidity control; and water damage protection.

Planning plans: plans must describe the security controls that have been implemented and the rules of behavior for those who have authorized access. Have in place your system security plan; rules of behavior; privacy impact assessment; and central management.

Personnel security: you must ensure that the employees and contractors are trustworthy and meet security criteria. Ensure systems are protected when the employees terminate or transfer. Here you would have your controls for: personnel screening; access agreements; and third-party personnel security.

Risk assessment: you must periodically conduct risk assessments of information security, and consider operations, assets, and individuals. Here you're looking at security categorization, which you tie back to FIPS 199 and FIPS 200; vulnerability scanning; and technical service countermeasures survey.

Systems and services acquisition: you must ensure that sufficient resources are available for security. Use a system development lifecycle. Restrict installation and use of software and Assess third-party security.

System and communication and protection: you must monitor and protect at external and key internal boundaries and Employ architectural designs.

Develop software life cycles and security engineering. You can consider things like: boundary protection; transmission confidentiality; cryptographic key establishment and management; session authority; covert channel analysis; denial of service protection; and security function isolation.

And lastly, System and information integrity: must identify, report, and correct flaws in information systems. Protect from malicious code. Monitor security alerts and advisories. Here you're looking at: flaw remediation; malicious code monitoring; information system monitoring; software, firmware, and information integrity; and predictable failure prevention.

While there are many controls in SP 800-53, there's also an audit document that parallels this and is called SP 800-53(a). This document also includes a number of controls. As a security framework this is an ideal document, whether you're a federal contractor or not. This document can help you secure your organization, particularly as you're looking at gap analysis. What controls do you not have in place that need to be implemented? It’s agreed that SP 800-53 is a daunting in-depth document but with wide-spread significant information concerning controls. Every control is metered by the risk level of low through high scenarios. There are a number of criteria that must be accomplished for SP 800-53 to be effective in the development of your security framework and essential for the implementation of controls in the risk environment you designate.

Once you go through the process of using FIPS 199, FIPS 200, and SP 800-53, you will have an extremely powerful security program!

Unit 12, part 3

The Defense Security Services (DDS) operates and maintains the National Industrial Security Program Operating Manual (NISPOM), and this sets the rules for industry's access to classified material. The requirements for systems that will capture, create, store, process, or distribute classified information are all listed in the NISPOM. These requirements include: an information security program; system security plan; IS Security manager; information system users; and assessment and authorization. Also included are: systems and services controls; risk assessment; personnel security; physical and environmental protection; configuration management; maintenance; integrity; media protection; incident response; authentication and access; audit and accountability; system and communication protection. So, if you are set up based on NISPOM and those provisions, and, certainly, if you've effectively implemented SP 800-53, I think you'll find you already have the controls in place, are effectively managing the risk, and are meeting the NISPOM requirements. Keep in mind, that's for classified material. You'll undoubtedly need to be at the top edge of your game to be able to secure your infrastructure sufficiently to handle classified information.

Executive Order 13587 - Structure Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information: it was established due to increasing cyber activity against classified systems. The order sought to ensure: interagency sharing; implementing of minimum standards for information security; emphasizing personnel security; protecting against threats and vulnerabilities; and providing policies and minimum standards for sharing

classified information. One of the keys here is that the government agencies must assign a senior official to implement the program.

Contractors must create an insider threat program. This means: implementing a capability to gather relevant insider threat information; establishing procedures for reporting an individual who poses an insider threat; deterring individuals from becoming insider threats; and mitigating insider threat risks. Contractors must: conduct an annual self-assessment and certification of their insider threat programs; establish a process that identifies negligence or carelessness in handling classified information; and establish insider threat awareness training.

Executive Order 13556 handled unclassified information throughout the Executive Branch that requires safeguarding or dissemination controls. In 2015, the Defense Department overhauled contractor cybersecurity rules and identified covered defense information. This is unclassified information that falls into one of several categories: controlled technical information; critical information; export control of unclassified information; and other information identified in the contract. You wrap all these things together, the Executive Order, and the covered defense information, and you have what's called Controlled Unclassified Information.

The categories are so broad that they cover virtually everything in the defense industry. The two primary requirements for these rules are: there must be rapid reporting of incidents and compliance with NIST security framework for sensitive, but unclassified information. You can look at NIST publication SP 800-171- Protecting Controlled Unclassified Information in

Non-Federal Information Systems and Organizations. This is again one of those documents that’s in the SP Section Special Publication Section on the NIST repository of documents. Again, there's a plethora of these documents out there, and certainly there are documents that are probably addressing some of the security concerns or security technologies that you're either looking to implement or looking to add to your system at some point in time.