DO YOU KNOW THE LEGAL ASPECTS IN CYBER SECURITY?

*Carla J. Miller Montroy  
University of Maryland University College  
2 Ren Roy Drive  
La Vale, Maryland 21502  
Cjmontroy.esq@gmail.com  
813-293-5502

Jian Hua  
University of the District of Columbia  
4200 Connecticut Avenue  
Washington DC 20008  
jhua@udc.edu  
202-274-7138

ABSTRACT

Today, every organization, whether small or large, is fraught with security vulnerabilities. Accordingly, organizations need the IT staff that is well informed and trained in the recognition, handling and legalities regarding security incidents. This paper discusses 10 legal aspects in cyber security domain. This research demonstrates to organizations that the adoption of some, if not all, of the practices associated herein would be considered industry best practices. Lastly, the current administrative legal controls are examined in light of the current and trending computing environment.

Keywords: Cyber Security, legal, regulation, networks

INTRODUCTION

The internet has led to the development of new types of crimes and more inventive ways to commit the old “traditional” forms of crimes. For example, some of the crimes that are aided by the internet are cyber stalking, identity theft, child pornography, fraud and scams, hacking, copyright violations, etc. (May, 2004). Most generally, when typical computer users think about their computing habits; ethics and legal regulations do not come to mind. Unfortunately, some in society are involved in various types of criminal behavior, blue and white collar crime alike, that do not exclude the use of a computer. Sometimes the computer itself is the target of the crime, other times the computer is the instrument of the criminal behavior.

In response to the overwhelming and expanding amount of cybercrime, the governing and legislative branches of our federal government have put forth some regulatory efforts to stymie the growth of the cybercrime arena. As a complement to the Federal response, the local governments have attempted to employ the use of some antiquated and some more recent criminal law statutes to punish the offenders. It is imperative that all IT professionals should understand prevailing legal conditions and security concerns.

An IT professional must be aware of the legal boundaries one has to work within in light of the growing trend of cybercrime. One must also be aware of the various legislative acts that one’s company must comply with. A cyber security professional must also be aware of how to protect and shield the company from liability with any alleged breaches of privacy and/or employee

*Corresponding Author
computer misuse. Additionally he/she must be equipped and knowledgeable with how to handle any and all incidents concerning cyber security, etc. and must precisely follow procedure.

Aspect 1: What are a risk, threat and vulnerability first and foremost?

A risk is the likelihood of a threat agent taking advantage of vulnerability, whereas a threat is known as any potential danger that the vulnerability will be exploited or exposed by a threat agent (Harris, 2010). A threat agent could be a regular person, a student, an employee, a hacker or any given number of individuals working alone or in collusion. There is also the threat-source which can either be an intended method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability (Stoneburner, Goguen, & Feringa, 2002). A vulnerability is a specific weakness in security (or lack of security measures) that typically could be exploited by multiple adversaries having a range of motivations/interests in different assets (Johnston, 2010).

Some new risks and threats include, but are not limited to, invasion of privacy, software, music and movie piracy, file sharing programs, theft of trade secrets, theft of data (computer criminal activities), email attachment viruses, and hackers’ activities, etc. The invasion of privacy could deal with students, employee or client privacy. Some of the activities that fall within the scope of hacker activities are social engineering, system intrusions, break-ins and unauthorized system access whereas computer criminal activities refer to some of the aforementioned crimes such as cyber stalking, information bribery, system intrusion, fraud, theft of trade secrets, identify theft, etc. (Stoneburner, Goguen, & Feringa, 2002).

The motivations behind the intentional behavior could be for such reasons as curiosity, ego and intelligence, monetary gain, revenge, rebellion, challenge, destruction of information, illegal information disclosure, unauthorized data alteration, etc. (Stoneburner, Goguen, & Feringa, 2002). As much as one may think that all criminal or illegal behavior is undertaken knowingly and intentionally, some of the behavior is not intentionally undertaken knowing that it is illegal. There are several examples of such behavior that is done by individuals without criminal intent, such as software sharing, selling a computer with the operating system still intact, making unintentional data entry errors or programming errors, downloading of copyrighted works, posting questionable information on Facebook or other social networks and cyber-bullying. Except in the situation of natural disasters, there are other common threats/risks (such as unpatched computers, weak passwords, rogue wireless access points, weak physical security, privilege escalation, phishing, disgruntled employee issues, etc.), an IT professional must be aware of. The IT professional must also concern her/himself with the related criminal acts of others, incident reporting, proper procedures, legal regulation and compliance, liability and other responsibilities of the like.

Aspect 2: What are the applicable laws and regulations in Cyber Security?

Administratively, the United States Government has attempted to regulate, protect and provide structure to cyber security and the criminal acts that occur therein. The laws that apply to cyber security, cybercrime and other criminal acts are multi-faceted and occur on different levels of an organization. There are laws that are aimed at prevention, others that are aligned with public
policy goals and deterrence laws that have jail time as their prescribed goals. The first applicable laws are the Federal Statutes and State Laws that encompass various requirements. The Federal Statutes, Laws and Regulations apply equally to all states. The administration of an organization must ensure that its employees are remaining compliant with the laws and regulations as the management is responsible for said actions (when the employee is performing in the scope of their employment).

There are other laws of the United States that are based upon common law and have two different categories: Criminal and Civil. This is not to say that the two kinds of law never intermingle, it simply means that for deterrence and reparations for wrongdoings, there needed to be two different categories. Criminal law is based upon common law, statutory law or a combination of both and accounts for public policy and/or public decencies in the consideration of same. Criminal law addresses the behavior that is deemed to be harmful to society at large, therefore punishment usually involves incarceration, rehabilitation, probation and/or monetary fines. Criminal law is commonly understood more easily than the second category of law, civil (or tort) law. Civil law is where the wrongdoer (defendant) owes a legal duty to the victim (plaintiff) due to a breach of a duty. The duty is usually measured against what a “reasonable person would do in the given situation” to prevent the harm to the victim. The damages can be financial loss, personal injury, or very likely a mix of both.

Each state has their own set of common law criminal and civil statutes that is governing in that particular state (in addition and separate from Federal Law Regulations, Mandates, Statutes, etc.). In some cases, the company could be held liable for damages if the employee was in the “scope of their employment” at the time of the infraction. The global trend is to hold company leaders accountable for non-compliance of the employees (Herold, 2006). Therefore, the IT staff and the management of the company/organization would have to make sure that they are familiar with the laws that apply to the state where they are employed, in addition to Federal Laws, and to ensure that all staff members are properly trained. Further, management will need to have all of the policies within the company pertaining to legal compliance narrowly tailored to ensure that the compliance language is clear.

Aspect 3: Should we concern intellectual property laws?

The administrative controls of an organization must be integrated with intellectual property laws. A past example of a large scale violation of intellectual property was the plagiarism of print books in the educational arena. However, with the progression of the Internet, electronic plagiarism and piracy quickly emerged and was embraced by diverse individuals. The United States copyright law protects the right of an author to control the public distribution, reproduction, display, and adaptation of his/her original work and covers many categories of work, such as graphic, pictorial, musical, dramatic, literary, motion picture, sound recording, etc. (Harris, 2010).

The Digital Millennium Copyright Act (hereinafter referred to as “DMCA”) enacted in 1998 amended Title 17 of the US Code prohibiting circumventing a technological measure designed to protect a copyright (May, 2004). DMCA also prohibits the removal or alteration of information identifying the author, copyright holder, performer and terms for use of a work for the purpose of
facilitating copyright infringement (Pepitone, 2012). An example of how DCMA regulates uploaded content is when a website has a user upload a protected song, video, etc., the owners of the protected content can contact the website to take the protected item down. At this point, the website notifies the user that uploaded the content of the removal of same in order to avoid liability. The user can counter the website and/or pursue court action in order to demonstrate that the item was not a protected item within DCMA and/or other copyright statutes (Pepitone, 2012).

Despite countermeasures in place in the form of copyrights, patents and laws governing same, the digital age makes abuse extremely easy and affordable (Bundschuh, 2004). The file sharing programs (ex: BitTorrent), CD-R’s to copy music, DVD-R’s to copy movies, shareware, and the misuse of personal software has made copyright infringement too easy for the regular lay person to engage in. Liability aside, many file sharing programs leave the computer and network vulnerable for attack, therefore the IT professional must be diligent in securing same. Another vulnerability is the exception to DMCA, which allows reverse engineering for the purpose of achieving interoperability among computer programs (unless forbidden by the software manufacturer) (May, 2004). The organization and the IT personnel employed therein should be concerned that malicious code could be injected into one of these programs under the guise of allowable exceptions under DMCA. The exception, while narrowly tailored, can still be exploited by experienced hackers in an effort to disguise their wrongdoing as “legitimate”. The DMCA, while being well intentioned, does not go far enough to prevent copyright infringement, both intentionally and non-intentionally. Therefore, the IT professional must be diligent to ensure that employees in their company are not using the company network or assets to commit infringements. This would include allowing users to copy such things as their “iTunes” library into the company’s computers and/or network or using Peer-to-Peer file sharing services. These programs not only open up the network to viruses and backdoors/Trojans, but also implicate the company as unknowingly aiding in the piracy of the employees.

In order to address the shortcomings of DMCA, the legislature has introduced alternative legislation in late 2011/early 2012 such as SOPA (Stop Online Piracy Act) and PIPA (Protect IP Act). SOPA was a bill proposed to aim at cracking down on copyright infringement by restricting access to sites that host or facilitate the trading of pirated content (Pepitone, 2012). SOPA aimed to cut off access to the pirate sites by requiring US search engines, advertising networks and companies to withhold their services to these locations (Pepitone, 2012). Lastly, SOPA imposed upon network, payment and advertising operator or company to set up a process by which outside parties can report to the company if one of its customer’s is an “internet site dedicated to the theft of US property.” (Pepitone, 2012). This act did not pass in Congress due to a critical and well-orchestrated opposition by major technology and internet companies within the US. However, watching upcoming and pending legislation is important for IT professionals to keep abreast of in light of his or her employer.

Aspect 4: Do you know the laws protecting trade secrets?

Trade secrets are information and resources that a company has that provides them with some sort of competitive advantage and is protected by law if developing it requires a special skill and/or expenditure of money and/or effort (Harris, 2010). Trade secret law covers a specific item or resource. In response to the theft of trade secrets in order to benefit foreign or domestic
individuals and/or companies, the Federal Government crafted the Economic Espionage Act (hereinafter referred to as EEA) in 1996 (May, 2004). The Act was created in order to stop trade secret misappropriation by making it a crime to knowingly commit an offense that benefits a foreign agent or government or to knowingly steal trade secrets or attempt to do same with the intent of benefitting someone other than the owner of said secret (May, 2004).

As the upper management of a company, it is absolutely imperative that there are policies put in place for screening employees, both current and future to evaluate the employee you are possibly hiring. It is imperative to monitor and provide training to employees on what is proper protocol and procedure within the company. While the media tends to focus on spectacular events, such as external hackers, employees inside an organization pose silent but more dangerous threat due to their intimate knowledge about the organizational systems and the permissions they receive properly or improperly (Hu, Xu, Dinev, & Ling, 2011). Therefore, it is absolutely vital for the IT staff to have the appropriate access levels in place to protect the trade secrets and to routinely review, scrutinize and test their security policies. Reason being, the legal field (especially Federal Law) is very complex and slow to amend. Accordingly, the law lags behind the changes in technology and the remedies afforded to breaches of same. As an IT professional, one must be diligent to protect the company trade secrets from outside and inside threats since the legal litigation response has the lag time.

Trademarks and Patents are some what related to trade secrets in that they are also encapsulated within intellectual property law. A trademark is used to protect a word, name, symbol, shape, sound, color, etc. whereas a patent is given to an individual or corporation to grant them legal ownership of and exclude others from using or copying the invention covered by the patent (Harris, 2010). IT staff and management of an organization must provide and accommodate for protection to the intellectual property of the company from any outside threat agents and internal threat agents (such as the disgruntled or rogue employee exercising privilege escalation, etc). As mentioned above, there may not be a readily available Federal or State remedy to cure or mitigate a breach. Additionally, legal litigation can be time and resource draining on a company (allowing for much public relations and other damage to be done to the company in the interval time while waiting for the litigation to resolve).

Aspect 5: Do we need to pay attention to and protect financial reporting?

Another realm of applicable laws is that of financial reporting. The company management is held to strict standards when it comes to financial reporting and the Sarbanes-Oxley Act. Sarbanes-Oxley Act of 2002 sets new and/or enhanced standards for all US public companies, however it does not pertain to privately held companies (O’Brien & Marakas, 2010). Much of Sarbanes-Oxley deals with accounting practices of companies traded on the public stock market, however there is a portion of said law that relates to Information Technology. The Sarbanes-Oxley Act aims for transparency and accountability by dictating how a company must track, manage, and report financial and other data. The IT professional is necessarily involved within the safeguarding and integrity of the data collection and preservation. For example, in Securities and Exchange Commission (hereinafter referred to as “SEC”) v. Shanahan, the SEC accused the corporate’s outside director of violations of securities laws via the use of backdating “in the money” stock options to corporate officers. 646 F.3d 536, (2011). The Shanahan Court
highlighted the importance of document security in regards to Sarbanes-Oxley Act by stating, “the Act of 2002 requires firms to disclose stock-option transactions to certain officers and directors within two business days...”. *Id.* However, by not disclosing in the proper time period, the company could be found liable. Therefore, since the above case disclosure within two days, the documentation and all transactions must be protected against any changes of date or other malfeasance to protect the company. The Sarbanes-Oxley act is imposed upon the management to insure that IT Professionals are aware of such requirements and protect all documents from being tampered with in light of any possible litigation.

Another financial reporting legal requirement is the Gramm-Leach-Bliley Act of 1999 (hereinafter “GLBA”). GLBA requires financial institutions to develop and disseminate privacy notices and allow customers the option to prohibit the institution from sharing the information with third parties. In the case of *American Family Mutual Insurance Company v. Roth*, the defendants were charged with misappropriating confidential information from AFM’s confidential policyholder files in violation of GLBA...by soliciting AFM’s policyholders to purchase insurance through the defendants..and tortuously interfered with prospective business expectations. 886 N.E.2d 1149 (2008). The *Roth* Court quickly clarified and noted that GLBA requires each financial institution to respect the privacy of its customers and to protect the security and confidentiality of those customers’ non-public personal information. *Id.* In no uncertain terms, the *Roth* Court stated that, “failure to comply with the GLBA may result in a cease-and desist order issued by the FTC, which could lead to, among other things, civil penalties of up to $10,000 per violation...” *Id.* Further, the *Roth* Court stated the GLBA was not enacted to benefit financial institutions; rather it was to impose special burdens and responsibilities on same. Accordingly, an alleged violation usually results in negative media and press coverage for the company (thus piercing reputation of company).

Obviously, the risk of financial sanctions is one aspect; however the risk of possible civil and/or other liability is another aspect that the management must take very seriously since same are possible remedies for a GLBA violation. The board of directors/management must implant and deploy appropriate policies then push said polices down through the ranks of the company. As such, part of the responsibility falls on the IT professionals, because the Gramm-Leach-Bliley Act requires that all employees be trained on security issues and protecting confidential financial information.

Additionally, an organization must be cognizant that there are many federal and state regulatory agencies that require information to be accessible for review and audit purposes. (Gatewood, 2009). Further, if same information has been used by the organization to report compliance activities, it is critical for the organization to show to the requesting agency that the information remains unaltered from its previous state (Gatewood, 2009).

The management of the company must work in concert with the IT professionals to institute safeguarding data measures and to review on a regular basis Access Control Lists, the Rule of Least Privilege, password policies and other practices as it relates to employee access to prevent unauthorized access, data modification or privilege escalation. Sarbanes-Oxley, HIPAA and GLBA all impose security requirements upon organizations. As such, an organization would
Benefit from implementing stronger security standards by allowing it to save money and time by avoiding multiple audits from multiple regulators. (Greene, 2011).

Aspect 6: What is the Computer Fraud and Abuse Act?

Naturally, there are laws regarding fraud that are not necessarily targeted at company management, but are nonetheless important for the IT professionals. The Computer Fraud and Abuse Act (hereinafter referred to as “CFAA”) was originally written in 1984 and later amended in 1986 and prohibits different activities and designates any infractions as federal crimes. It covers such activities as the following: knowing access of computers of the federal government to gain confidential information without authorization; the intentional access of a computer to obtain information from a financial institution without authorization; intentional and unauthorized access of computers of the federal government; the knowing access of a protected computer without authorization or in excess of authorization with the intent to defraud; knowingly causing the transmission of a program, information or code and as a result of conduct, intentionally causing damage without authorization to a protected computer; the knowing trafficking of computer passwords and the transmission of communication containing threats to cause damage to a protected computer (Harris, 2010). Further, the statute criminalized unauthorized access that damages a protected computer even if the intruder did not intend (or have the requisite mens rea) to cause damage to same (Ena, 2008). The statute was amended to include crimes that involved computers and enhanced sentences for crimes committed with the help of computers (the Federal Sentencing Guidelines allow longer sentences for defendants that used special skills—including the use of computer skills) (Ena, 2008).

There have been successful federal prosecutions under CFAA in the past. For example, in United States v. Phillips, the former University of Texas student violated the University’s acceptable use policy and gained unauthorized access to governmental and private computer systems (he accumulated a large amount of proprietary information and caused numerous crashes to the University computer system) (Ena, 2008). Eventually, the Secret Service became involved and apprehended Phillips. The case went to trial and Phillips was found guilty of Computer Fraud under CFAA and sentenced to five years probation, five hundred hours of community service and restitution over a $170,000. Another example of successful prosecution occurred from an insider breach at a debt collection company. In United States v. Willis, the Court upheld a conviction under CFAA against an employee of said agency that provided criminals with access credentials to LexisNexis Legal Research Website, which enabled the criminals to commit identity theft and credit card fraud (Ena, 2008). It was found that the “rouge” employee was the sole individual responsible for the breach and violation of the basic information security principles (even simple principles as account activation and revocation).

The management of a company must train and impress the importance of compliance upon the staff. Additionally, security training is required for all IT staff on how to recognize any suspicious behaviors. A zero tolerance policy must be instituted and practiced by management and the IT department regarding any wrongdoings in relation to cyber crime, employee wrongdoing and CFAA in order for the company to pursue compliance. For example, In the case of Phillips mentioned above, one could easily conclude that the University of Texas grossly mishandled the numerous violations by its undergraduate student. The University’s Information
Security Office learned of the activities of the student and issued several warnings but stopped their action (or engaged in inaction) at that point. Further, to add to its gross mishandling of the situation, the University admitted the offending student to the graduate computer science program (Ena, 2008). In the above mentioned case of Willis, it would appear that the company did not have the proper credential and background checking procedure in place. Additionally, the rogue debt collection agency employee had access to revoking and creating credentials on LexisNexis, an act that was most likely outside the scope of her employment. The employer could have been more vigilant in monitoring for said behavior.

Aspect 7: What is the Anti-hacking Statute?

The anti-hacking statute was amended and reinforced in 2002 by the Cyber Security Enhancement Act and Homeland Security Act. The new Act broadens the scope of law enforcement and governmental agencies to allow them greater access to ISP (internet service provider) communications if the ISP believes criminal activity is a foot. The ISP is allowed to release any information if they believe criminal activities are taking place without the need of a warrant. This could lead to serious problems for a company that is not being prudent in their security and computing practices. If the ISP chooses to disclose a company’s traffic, there could be serious implications and harm come to a company due to the activities of an individual or group of employees. The IT staff must exercise due diligence in monitoring and screen their company’s IP traffic and employee computing activities to mitigate the chances of employees engaging in computing practices the ISP would flag as suspicious. Additionally, if there appears to be a large amount of illegal or questionable traffic coming from the IP address that is associated with the company, the company may be subject to further evaluation and public scrutiny.

The Computer Security Act of 1987 was enacted to “improve the security and privacy of sensitive information in Federal Computer Systems” (Poffenberger, 2004). The law requires every government computer system that contains sensitive information to establish a security plan and provide periodic mandatory training for all persons who manage, operate or use these systems (Poffenberger, 2004). This law also names NIST (National Institute of Standards and Technology) as the agency responsible for the vulnerabilities of Federal Computer Systems, for developing standards and providing technical assistance (Poffenberger, 2004). As an IT security person within a governmental entity, he/she is expected to help the employer to avoid incidents like the recent Wiki Leaks scandal.

Aspect 8: Are there any laws protecting organizational privacy?

There are numerous laws that cover privacy issues from law enforcement actions to management actions and basic general protections. Many previous laws were passed, such as the federal wiretap law, however many became outdated and had to be revised. In 1986, the Electronic Communications Privacy Act (hereinafter referred to as ECPA) made it illegal to intercept stored or transmitted electronic communications without authorization and set out the provisions for access, use, disclosure, interception and privacy protections of the electronic communications (May, 2004). The management of a company must be aware of this act and not capture or inspect their employees email or web traffic without the proper precautions put into place.
Examples of said precautions are security and acceptable use policies, warning banners on login screens (on the company machines) and signed waivers from employees waiving their right to privacy on company telecommunications equipment and bandwidth. The management is permitted to monitor their employees, however, it must be work related and applied non-discriminatorily.

Another related law that deals with privacy and the level of security exercised by a company is Heath Insurance Portability and Accountability Act (hereinafter referred to as HIPAA) enacted in 1996 that established a broad array of privacy and security rules to create safeguards against unauthorized use or disclosure of medical records (O’Brien & Marakas, 2010). In particular, the security rules pertain to Electronic Protected Health Information (hereinafter referred to as “EPHI”) and incorporate three types of security safeguards that are required for compliance: administrative, physical and technical. Any violations or misappropriation of private health information could result in serious sanctions, violations and liability for the company. The violation would apply whether in paper document format or electronic format. HIPAA requires covered organizations to establish adequate safeguards that address and ensure the privacy of protected health information (Herold, 2006).

However, as previously noted, Congress has been more cognizant of Cyber Security issues and the importance of private data. Accordingly, a bill was drafted this year, aptly titled, “The Cyber Security Act of 2012” (hereinafter referred to as “CSA”) that is aimed at the protection of critical infrastructure systems (Aitel, 2012). This bill, in essence, aims at protecting critical infrastructure systems in the US by focusing on the sharing of information and private user data between companies and the government (Aitel, 2012). The bill labels critical infrastructure systems (including financial systems) as new cyber war battlefields and requires them to upgrade to military-style defense (Aitel, 2012). As an IT professional employed in any of these critical infrastructure system companies, he or she must be abreast of the legal requirements that may come through from the legislature. The IT professional must also keep up to date and ensure compliance of the requirements imposed on said companies for sharing of private user data. Liability could be imposed for the misappropriation and dissemination of private data if not handled correctly. This bill, to date, has not passed. However, it is likely that this or an updated version of said bill will be proposed and possibly passed in the future.

**Aspect 9: What are administrative and technical safeguards?**

As one can see, there are many Federal Laws that one must follow as well as the applicable state laws that serve as administrative controls for management and an information security professional. Additionally, it should be reiterated that the laws do not keep up with the changing face of technology and may not provide the protection a company would hope for. There are some administrative and technical safeguards that can be done by the IT professionals in mitigate the risk to the company.

There is a non-mandatory administrative control that is imposed upon IT professionals by the Computer Ethics Institute that is advisory in nature. This control is referred to as the Ten Commandments of Computer Ethics and contains such rules as one shall not use a computer to harm another. (Computer Ethics Institute, 1992). It would be a good and cost effective idea to
have all staff (IT and non-IT) trained on these ethics and to have same posted in open, obvious locations.

Administratively, a necessary stance for management and an information security professional to take is to mandate cyber awareness training for all employees. Training related to security, ethics and cyber safety should be mandatory and done on a regular basis. Employee competency testing, as it relates to the training, should be conducted. Additionally, there should be an ethics policy developed in addition to the security policy that outlines ethical computing behavior and expectations that is posted and distributed to all employees. As previously mentioned, the employee must know what the limitations are to their privacy on the organization/company computers and should sign a waiver. Absolutely no expectation of privacy should be granted, promised or conveyed to the employees. A security policy is necessary that spells out that there is no expectation of privacy on work computers, materials, company resources, etc. Warning banners should also be visible on company computer logon screens.

Administratively, the organization must be diligent in potential employee screening processes. The company should look for employees that have a high level of self-control and strong moral beliefs for sensitive positions and assign employees with lower self-control to positions wherein they are not custodians of sensitive information (Hu, Xu, Dinev, & Ling, 2011). This could include using psychometric instruments for testing to ensure that the strong self-control individuals are selected for the most sensitive positions (Hu, Xu, Dinev, & Ling, 2011). The company also should adopt high standards for ethical behavior of its employees and foster corporate citizenship in order to attract the preferential employees.

The company must exercise due care and diligence in dealing with their security to prevent any breaches. In response to exercising due care and diligence, an incident reporting/handling procedure and protocol should be put into place to handle breaches. An incident response team, as part of the company’s policy, should exist to respond to any and all possible security incidents and have a chain of command established. The company must stipulate a systematic way of having this team respond and handle incidents. The company could also employ an in-house or on-call as needed a computer forensic expert to assist the incident response team to fully investigate any incidents. One key to a company having a successful incident response policy is also making sure that they hold individuals accountable for their actions and ensure no reprisals for any employee reporting (Bundschuh, 2004).

The technical safeguards and controls that can be employed vary given the environment. For example, in any given environment, the IT staff should know their systems. This would include knowing the details of the networks, printers, hubs, routers, and workstations, knowing all configurations and having a network diagram/map. Additionally, the IT professionals should be familiar with the entry points of access, the running services and associated port configurations, know all of the hardware and software on systems and perform a risk assessment (Poffenberger, 2004). A network architecture diagram and/or map should also be kept on hand for reference. Another technical safeguard that would be prudent to employ is the practice the principle of least privilege and “need to know”. The principle of least privilege in computer security refers to granting an employee the smallest amount of privilege necessary to perform their job duties. This principle should be employed on all systems and updated frequently (especially critical
when an employee leaves). The privilege of “need to know” refers to granting an employee access to resources only if they have a realistic and actual need to have access to said resources. Additionally, all steps for adding, modifying, or removing users to the system and granting, modifying, and removing privileges of users should be documented (Poffenberger, 2004).

Other technical controls that should be employed to aid in legal compliance are included in practicing “defense in depth.” Defense in depth includes, but is not limited to, the use of some hardware and software items such as of firewalls, identification, authentication and authorization, encryption, separation of servers and duties, routers and switches, system monitoring, installation and maintenance of patch and upgrades and hardening of the operating systems. Simply put, firewalls are the first layer of security that control who and what has access to the network and can be nested inside and outside of the network (Poffenberger, 2004). Identification, authentication and authorization work in conjunction with each other in that each user must have a password or some other authentication token to be authorized to use the system. All data crossing the network to one or more databases or to the internet should be encrypted. Routers and switches also aid in keeping out traffic in conjunction with an access control list that can include known hacking addresses. The IT director and/or staff should monitor the network and system with intrusion detection equipment and with any other equipment that can aid in monitoring traffic patterns. All antivirus, Windows and other updates should be pushed out system-wide to the workstations and done promptly. Lastly, all the systems should be hardened per best practices standards (removal of guest accounts, changing of default passwords, etc.). An IT Professional should also be skilled in conduction penetration and intrusion detection to discover vulnerabilities to ensure that the company is able to remain compliant with all of the administrative legal controls that management is charged with.

Aspect 10: How much are the costs associated with the Legal Controls?

The inevitable question that crosses the mind of many at this point is how much will this cost the company? It is very difficult to say the costs that are associated with these controls. In regards to the training element, it comes down to the cost of staff hours for developing a training and policy program and training the staff on same. In regards to the hardware, technology, software, etc., it would really depend on the size of the organization, data to preserve, mission of the organization and classification of same. Obviously, a governmental organization has higher requirements to comply with and hence, spend more on the technology and security budget to remain in compliance with NIST. A smaller company or organization are concerned with their budgets and have to keep cost savings and cost conscious decisions in mind. A medium or larger size company will have to take into account their current size of IT staff as well as current inventory and abilities in order to make an educated decision. The cost could range from a few thousand to several thousands. A quasi-governmental organization (such as educational institutions) could easily spend hundreds of thousands of dollars on the system to remain in compliance with the administrative controls associated with educational institutions (such as HIPPA and FERPA).
CONCLUSION

In conclusion, an IT professional must be kept abreast and aware of the legal changes and challenges in society as well as the changing technology. It is simply not effective, realistic or a best practice for the IT professional to be skilled in the technical aspects of technology only. Additionally, since technology is constantly evolving, the law must evolve to keep up or to at least meet the demand. As the law evolves and grows, the company will have to expend money and resources to stay abreast of changes and to remain in compliance. As technology advances and makes it easier for attacks and for the occurrence of cyber crime, the need to protect the data and trade secrets becomes even more imperative.
REFERENCES


