Analyzing Security at Firion Corporation and Suggested Security Policies

Blue Team
Marcus Guevara
Sammy Wong
Shanaun Clayton
Dave Shields

Submitted to Dr. Michael Hanners

In Partial Fulfillment of CSEC620

University of Maryland University College

Table of Contents

Abstract

The purpose of this paper is to create a policy that will ensure Firion's compliancy with governmental regulations concerning cyber security as well for the protection of the company and its customers.

Introduction

Firion is a corporation which develops, produces, and markets specialized jackets used in waste disposal and other safety-related applications. Like most modern companies, Firion utilizes technology for increased efficiency in production, networking among employees, and to store and maintain important data. For example, databases contain employee and customer information as well as sensitive information about the research concerning Firion's new glove designs and coatings. It is of extreme importance that Firion be able to keep sensitive information confidential to prevent loss of financial interest through lawsuits or loss of profit. If Firion fails to keep certain information confidential the loss of employee and customer confidence in the company and the potential loss of technological edge over competition can be extremely damaging and difficult to recover from.

Recent cases of hacking show how common cyber-attacks have become and help stress the importance of taking steps to prevent Firion from being a victim of such attacks. Epsilon, "the largest email marketing service company in the world" fell victim to an attack in early March of 2011 (Business Insider, 2011), and Sony was dealt a huge blow the very next month when about 70 million of their customer's credit information was compromised (Business Insider, 2011). Lastly, in June of 2011 Google announced that Chinese hackers had compromised the Gmail accounts of U.S. politicians using an attack called Spear Phishing (Business Insider, 2011).

These major attacks happened within the span of a few months and there continues to be cases of attacks like the ones listed above. There are very serious repercussions for a company if they are attacked in such a manner as Sony. For example, PlayStation users in New York filed suit against the Sony claiming negligence (McEntegart, 2011). In order for Firion to protect its self against these and other attacks, there must be a sound cyber security policy in place in order to ensure that the company is actively protecting its own interests in all the necessary areas.

In order to have a complete cyber security policy, Firion must take into account two major issues: compliancy with federal laws and regulations and protection of the company's interests against cyber threats. The U.S. Government has enacted several laws that companies must enforce in order to better ensure the security of their own company as well as the security of its customers which are likely to be U.S. citizens. So it is in the best interest of Firion to ensure that such laws are enforced to increase the security of the company and to decrease Firion's liability as well as avoid potential fines. Secondly, it is important for the cyber security policy to dedicate proper examination of the human aspects which affect a company's security and provide practical solutions to each human vulnerability or threat. It is of first importance to protect Firion and its employees and customers but that protection should not stifle Firion from being able to conduct normal business. In the end, the aim will be to create a cyber-security policy for Firion which addresses all the necessary issues and retains a balance of sufficient security without over restricting the business.

Federal Compliancy Laws

Regulatory compliance is an important part of business no matter how large or small, ensuring that employees take all steps required to follow laws and regulations is vital.

Violating one regulation, however small it may seem, can result in fines and other repercussions. Regulatory compliance covers a wide range of rules. Numerous government legislation acts exists that provide the regulations that all companies must abide by. It is important that compliance standards are met, as it will serve to protect employee and customer personal information from access by unauthorized parties. Failure to comply can lead to fines, imprisonment, or both.

Federal Information Security Act (FISMA) is a legislation signed into law as part of the Electronic Government Reform ACT of 2002. FISMA describes a broad context to protect sensitive information from man-made and natural threats. FISMA makes permanent the information security management responsibilities introduced and delegates assignments to several agencies ensuring that all data is secure. The act requires that agency officials keep risks low or at satisfactory levels. The National Institute of Standards and Technology (NIST) define the actions toward fulfillment with FISMA to include:

- Risk Assessments
- Security Awareness Training
- Policies and Procedures
- Security Plans
- Contingency Plans
- Incident Response Procedures
- Remediation Procedures
- Annual Security Testing

Since the establishment of FISMA, Federal information systems and databases have been integrated into non-Federal agencies, including law enforcement, and businesses (NIST, 2010).

The Health Insurance Portability and Accountability Act (HIPAA), provides regulation for the use and release of an individual's medical information. The goal is to guarantee that an individuals' healthcare information is secure and still permitting the flow of healthcare information that is necessary to protect the public's welfare and boost the quality of healthcare. HIPPA established a standard that allows important use of the information, while protecting the privacy of those who seek medical care (Summary of the HIPAA privacy rule., n.d.).

The Sarbanes-Oxley Act (SOX) was introduced in 2002 in response to the Enron and WorldCom scandals. The Sarbanes-Oxley Act is organized into eleven sections and is designed to prevent financial fraud from errors in accounting or fraudulent practices. IT and financial departments are affected due to the fact that IT departments have the daunting task of having to produce and preserve an archive of corporate files in a way that is lucrative and that complies with the requirements set forth by the legislation. SOX states that all records can only be saved for five years and allows enough information about transactions to be made available that allow one to identify where misstatements due to fraud or human error could occur. The SOX Act makes available information and controls set forth to detect or prevent fraud (What is sox – sarbanies oxley act., 2010).

Some other critical legislation impacting the security of Firion include the Electronic Communications Privacy Act (ECPA) and The Digital Millienimum Copyright Act (DCMA). The ECPA prohibits a third party from disclosing or diverting communications without proper authorization. The law was enacted in 1986 to cover a wide array of electronic communications. It also forbids the unauthorized access and particular release of communication content and protects communications in transit as well as in storage (Federal statutes, 2012). The DMCA protects the rights of copyright owners and consumers. The controversial reform covers circumvention of copyright protections, fair use of copyright materials, and protection of ISPs from liability as long as they follow specific procedures. DMCA also forbids bypassing of access controls, copyrights, and bans devices, which does circumventions. The act is considered to be a compromising measure because it would prohibit activities that are ethical. Revisions have been made to DMCA to allow encryption and security research (Rouse, 2011).

Potential Threats

There are several threats to Firion's security and infrastructure. These are both technical threats and human related threats. All of these threats affect the confidentiality, integrity and availability of the information systems in use at the company. If left untouched, these threats are likely to have a significant financial and business impact on Firion.

Based on Firion security review, there are two technical threats that can affect Firion’s security and privacy goals. The first technical gap is the lack of change control on critical systems. In the incident where Nina was able to disable the ports on the firewall without any special permission is an indication that no formal change control or detection system is in place. The firewall incident also shows lack of separation of duty in Firion’s IT organization. With no separation of duty and change control, there will be very little monitoring of infrastructure to detect any abnormal changes. This threat allows attacks from both inside and outside Firion to be difficult to detect. The lack of change control also extends to the client desktop environment as in the case of Lloyd, the HR manager, who was able to change his computer settings without any challenge. A user having administrative rights on their machine is one of the leading causes of virus and malware infection. With the current state of security at Firion, hackers or cyber criminals can conceivably open ports on firewalls and redirect traffic to and from the internal network with minimal detection or restriction.

All the criminals need to do is to obtain a user’s credentials and they may be able to perform changes on the network infrastructure. The potential of a denial of service attack (DOS) on Firion’s domain name services (DNS) records could cause a large outage of the Firion infrastructure. In order to combat this technical gap, Firion requires a formal change control and review process. By combining separation of duty and a proper change control process, the risks can be greatly minimized and issues can be detected in an earlier stage.

The next technical threat is the lack of content filtering for Firion web and email traffic. The ability to block unauthorized or even dangerous downloads is an important factor in securing Firion endpoints. We need to have the ability to monitor and filter web and email traffic to and from Firion’s network. One of the attack vectors of virus and malware are from active web content on websites (Tittel, 2005). The absence of download protection and change control on user computer will open Firion’s computers as a target for advanced persistent threats (APTs). These APTs could be infecting Firion’s infrastructure and stealing data. The potential loss of intellectual property could cost Firion billions of dollars in damage and unprecedented reputation damage. According to a Verizon Data Breach Investigation report in 2011, 49% of data breaches are caused by malware (Verizon, 2011). The Internet also is a prime area for reconnaissance and social engineering of target such as Firion. In one incident, Chinese spies using a fake Facebook account for social engineering were able to obtain user information and threats such as this cannot be ignored (Chinese Spies Use Fake Facebook Pages to Gain Intel, 2012). By implementing a defense in depth approach, Firion will ensure all end-points receive maximum protection against the ever changing threats from the Internet.

Additionally, Firion has two major security threats that are related to its employees.

The lack of a formal acceptable use policy (AUP) does not give users or management any guidelines regarding the daily regulations needed to secure the Firion infrastructure. The incident involving Laura requesting trial software without getting proper security review and authorization shows the lack of security awareness and formalized procedures for requesting an exception. According a report from Ernst & Young, over 75% of security breaches are caused by activities by internal users (H. M. P. S. & Wijayanayake, 2009). Misuse of computer resources in the workplace not only reduced productivity of the users but also bring additional risks to the company's reputation. Activities like surfing the web and participating in social networking sites might bring questionable content to the workplace. In the case of the Melissa virus, created in 1999, it was originally planted in an alt.sex Usenet newsgroup message. The billions of dollars of productivity loss and the negative publicity a similar breach produces can tarnish the image and the business interests of Firion. Without a formal review of software requests, the IT security organization will not be able to design a security solution to cover the user base. This gap could allow both internal employees and external intruders to plant malicious software such as Trojans on their machines that may disrupt services or steal data.

The most serious of security threat to Firion is the risk of data loss. The incident of Nina stealing R&D data from Firion should serve as a wakeup call of the state of security. The advent of Web 2.0 and social networking makes it easy to share information across many different sources and media. This new Internet environment also makes it easy for personal or corporate information to be leaked to the Internet. In the case of Sandra blogging on the Internet during business hours, it might be improving communication and collaboration with customers but at what risk? The lack of controls on the flow of information makes it difficult to safeguard company data.

The primary use for Web 2.0 from a corporate standpoint is improving communication both internally and externally. The primary concerns with this method are the security issues it could create and the potential for sensitive company information to be made public (Donston, 2008). If a web filtering solution were implemented at Firion, and education regarding data classification were provided to users, the risk of critical business data leaked to the Internet accidentally can be greatly reduced.

Another vector for a potential data loss is the emailing of information to an external email account. The incident involving the development manager Sam Elliot demonstrated that data could be leaked to an external source with little or no knowledge of the IT Team at Firion. Once data is stored in third party storage, Firion loses control of the storage and backup of the data. For example, once the data is stored with Google, Google will have complete control of the data and may choose to allow the data to be searchable from the Internet. Imagine if company intellectual property was accidentally emailed to Gmail and its servers determined it should make the data searchable on the Internet. The leak of such information might cost Firion billions of dollars in sales and greatly hurt its image.

There are industrial spies and cyber criminals constantly searching the web for any information that they can sell for a profit. The last data loss vector that Firion faces is the use of removable storage. Removable storage devices such as CDs and USB drives are getting smaller and smaller. It is easy for user to misuse the media and open the company up to potential data loss and most of these storage devices do not employ encryption making the data an easy target for anyone to steal and copy the information. Incidents like Countrywide Financial Corp losing 2 million customer applications for mortgage due to an employee copying them to a USB thumb drive (Reckard & Menn , 2008) are perfect examples of the threats these devices pose.

Filling in the security gaps require the security organization to take on a multi-prong approach. First of all, having a data classification policy and the appropriate control measures ensure critical data is properly identified. Once we identify the critical data, we can design our solution to protect data when it is at rest or on the move using technologies like encryption. Secondly, having a data loss prevention solution to monitor web, email and removable media access is a key factor to reduce data leaks. We need to have a solution that covers most of the common exit points of data, flags the channels where sensitive data may be stored and allows us to take action to remediate loss.

Lastly, having an acceptable use policy and properly communicating and educating the user base will ensure proper security control will be executed. We need to address the widening socio-technological gap that happens in our modern workplace and need to give guidance on how to apply ethical behavior in the workplace. The traditional security policies and acceptable use policies were focused on deterrence, however modern ideas suggests that having the acceptable use policy designed in such a way that it gives users a sustainable ethical decision making structure (Ruighaver, Maynard, & Warren, 2010). We want the user to be aware of the consequences their actions may have on the company and encourage them to make an ethical decision on the use of company resources while considering security as a personal responsibility.

Firion Policies

Acceptable Use Policy

By the very nature of the works which are performed at Firion Corporation, there are a great many trade secrets, development data, sales data and other private data. These items are greatly prized by our competitors and if one data breach were to occur, it could cause a considerable amount of damage to our competitive edge (Kabay & Takacs, E-Mail and Internet

Use Policies, 2009). As a result, Firion has now created the following terms for the acceptable use of all information systems and company property. All employees wishing to maintain their employment with our company shall be bound to these policies from the date of which it has been received.

This policy applies to Firion Corporation, its parent, all subsidiaries and affiliates which we will now refer to as the "Company." This policy is used as the guidance for the acceptable use of the Company's various technological resources including telecommunications devices, Company access to the World Wide Web (WWW), LAN and WAN, electronic mail (email), mobile devices, and any other item so deemed as company property which is wholly owned by the Company. As these items are provided to the employees of the Company for use, they are property of the Company and therefore no guarantee of privacy or personal ownership of any usage or data stored on them including but not limited to email activities, web accessible resources, and any document or creation made possible by software which has been added to the system (Kabay & Takacs, E-Mail and Internet Use Policies, 2009, p. 48.24).

All Company assets shall be configured by the Firion IT department to meet the standards set forth in the IT configuration baseline and no modifications may be made to hardware or software on the asset without approval from the IT management team. It is therefore, not acceptable for Firion employees, contractors, vendors or business partners to install software such as any "freeware" or "shareware" applications nor to install trial versions of any particular software regardless of whether or not the full version is in use by the Company on its assets. It is also not acceptable for any employees to install any hardware that they have personally procured into their machine including RAM, hard drives, CD-ROM drives, monitors, or other peripherals not expressly purchased by the Company.

Internet usage and access to the WWW from the Company's resources is a privilege designed to aid employees in their productivity while enhancing the Company's competitive edge. However, this resource may be easily abused and thusly all employees must agree to the following terms when using the Internet. Due to the highly public and relatively insecure nature of Social Networking sites including Facebook, Google+, MySpace, and LinkedIn, access to these resources from within the Company is restricted and heavily monitored with various technical measures (Bamnote, Patil, & Shejole, Social Networking - Another Breach in the Wall, 2010, p. 152.). When an employee is using privately owned devices such as mobile phones, tablets, and personal computers to access these sites they agree to omit the Company from any mention on these sites including financial data, building information, projects in process and anything else pertaining to the Company and its operations.

All Internet access using the Company's resources should be used for business purposes only and employees using the Internet agree to monitoring of data usage including websites visited, duration of visit, types of data visited on the Internet and more. In order to protect its assets and valuable intellectual property, the Company has full control over Internet usage with no expectation of privacy either expressed or implied. Some personal usage of the Internet is permissible by the employees of the company provided the usage thereof does not impact productivity nor violate anything expressed within this AUP or any applicable state, federal, or international laws.

As with social networking sites previously mentioned, employees of the Company agree to not post or otherwise make publicly available any information regarding the Company and its activities on these systems. Furthermore, no employee shall publish information about the company on their own personal blog, web portfolio, or personal website.

In the event that data has been posted to the Internet without the Company's consent, those responsible agree to remove any and all data at the sole request of the Company at their own expense. If any information is found to express information that could be considered 'insider information' or otherwise libel or slander the Company, the Company reserves the right to pursue these crimes in the court of law and may discipline employees responsible up to and including termination of employment (Kabay & Takacs, 2009). Any employee wishing to post information about the Company on such a site must first receive approval from the Communications director and may likewise require that the data they wish to present is approved by the CISO.

In order to reduce the chance of data loss and to prevent involuntary introduction of malicious code into the Company IT Infrastructure, access to and use of devices with removable storage including USB 'stick' drives, external hard drives such as those connected with USB, FireWire, or eSATA, and CD's/DVD's of the 'rewritable' variety shall not be permitted to connect to Company owned assets unless specific procedures are followed. Should business needs require the use of such a device, the employee must first request approval from the IT Security team and must have the device scanned by an approved individual using an approved scanning tool such as the Company's selected virus scan software. If a malicious code is released on the network without following the aforementioned procedure, the Company then reserves the right to determine the root cause of the breach and if traced to an employee, full disciplinary action may be undertaken up to and including termination of employment.

The Company itself also has certain acceptable use policies and guidelines with which it must govern itself in order to protect the data that has been entrusted to it and the protection of all data in order to remain innovative, progressive, and profitable.

The Company will engage in a corporate-wide asset management and change control policy in which it will create a series of baselines of ‘nominal behavior’ of the business computer systems and equipment. This change control will also be extended to business processes and procedures so that assessing the impact of a change on any particular element will be fast and simple. The Company has assigned a Change Control Committee who will be responsible for managing change across the Company and includes people from multiple business units to provide a clearer assessment of the impact of such changes (Kabay & Robertson, 2009, p. 44.2).

The Company has also created an Access Control Policy based on the Role-Based-Access-Control (RBAC) model to protect the access to its various resources (Goodrich & Tamassia, Introduction to Computer Security, 2011, pp. 23-24). Using this model, access to data as well as access to physical sections of the facility will be based on the role of the person requesting the access. Only those with a need to access certain data will be permitted to that data and those who do not need access to that data will be prohibited from said access. This is designed not to alienate the employees of the Company but rather to provide more safety to the data that is being accessed and to prevent unauthorized modification of that data. Additionally, in high-criticality areas such as the Company datacenter, only authorized employees will be permitted to access this facility.

In the event of a major disaster in the offices wherein the Company resides, the Company has also agreed to the creation of a Disaster Recovery Plan (DRP). In the DRP, the Company has created a series of roles and responsibilities for various employees to aid in the transition to our warm DR site.

As outlined in the DRP, the company shall have their full operations resumed in approximately 4 business days in order to resume responsibilities to our stakeholders and customers (Miora, Disaster Recovery, 2009, p. 59.20). For any questions or concerns regarding the responsibilities of the employees in the DRP, please contact the CISO.

As outlined previously in this AUP, all employees of the Company agree that acceptance and practice of this AUP is agreed upon to maintain employment. In this same way, the Company agrees to maintain proper change control, access control, and disaster recovery as conditions of this AUP to the stakeholders. All employees found to be in violation of this AUP will be subject to investigation and disciplinary action up to and including termination. The Company reserves the right to make changes to this document at any time provided that all employees receive notice of changes to this plan.

Data Classification Policy

Firion's information systems contain hundreds and thousands of hours of research data regarding its products. It is essential to safeguard the entire system for the life cycle of all the data it contains. An effective data classification policy will allow users to identify, label and design processes to handle company data (Kopp, 2008). The first portion of the Firion data classification policy should include a mission statement regarding the security goals. We need to enforce the concept of "need-to-know" to Firion's employees. Also, this will be a good portion of the policy to explain the "why" to the employees. We need to embrace the new paradigm of empowering our employees at Firion to make the right ethical decisions rather than focus on the model of punishment (Ruighaver, Maynard, & Warren, 2010). We can explain the use of the system and how it will facilitate business activities to help lower the cost of maintaining data.

We also can state that the risk of having a data breach will not only cost company financially, but also its reputation.

Our second section of the data classification policy will start addressing what constitutes “data” and “information”. We need to give employees a clear guideline of how data and information are defined. We also need to enforce the idea that data needs to be protected both at rest and in motion. In this section, we can emphasize the ownership and responsibility to the users and empower them to take the correct action when working with data.

Our Third section of the policy is to define security labels. The labels allow us to clearly classified information and how we can control its access. In the case of Firion, three levels can be used:

- Public
- For Internal use only
- Confidential

For each data classification, we need to address the definition and some examples of the data. This allows users to have an easy reference to the data they work with every day. For example, research data is automatically classified as confidential data whereas a company memo is only classified as for internal use only. Also included in this section can be an explanation to the user of the legal ramifications of data loss. This will also be a good place to tie the classification to any legal obligation (PCI, HIPPA or SOC) that the company needs to be in compliance with. During this process, the company must have a clear sense of the data flow and its processes. This policy combined with our understanding of Firion’s IT environment, will help us to determine the necessary technical controls of the data and user’s education needs.

Security Awareness and Firion

As part of the ongoing need to make all our people aware of the many security issues we face in the modern world, Firion will begin to implement many new security awareness tools to improve the employees' overall grasp of the many challenges we face. It is not enough to simply make sure we do not write passwords down on paper or to lock computers when not in use. There are many threats including social engineering, phishing, and internal threats that must be addressed in order to improve the security posture of the company (Raman, Baumes, Beets, & Ness, 2009, p. 19.17). As a result of this, the IT Security team has agreed to undertake several new tasks to improve personal security and operational security including the implementation of a security awareness program and creating a new security incident and response systems to manage security vulnerabilities within the organization.

In an effort to improve awareness of security, the IT security team is implementing a security awareness and training program that will provide training to improve understanding of security concepts and information sharing methods including the distribution of information to those in need via email updates or corporate website updates (Rudolph, 2009, pp. 49.28-29). Additionally, the team plans to launch an incentive system for employees showing concern for proper security initiatives. To improve training, the security team will be working in tandem with our creative department to create a security awareness 101 video that will be required as part of the onboarding of new employees and part of the personal completion goals for the existing employees. The video will be a helpful and informative video to explain the basics of our data protection initiatives and provide multiple opportunities for self-assessment of security knowledge. As new technology threats arise, the security team will make the information regarding these threats accessible to all employees in a concise and informative explanation. Lastly, a great security program is only as successful as the employees it impacts will allow so the security team will also work with our creative department to create an incentive system to reward those who aid in reporting security concerns in compliance with the security policy which may include individual notoriety or coupons for reduced prices on various goods and services (Rudolph, 2009, pp. 49.32-34).

While the internal security of the organization depends a great deal on the employees who are part of it, the external security and the operational stability of the organization depend a great deal on the work of the employees in the IT Security department. Although Firion already provides the latest security patches for Operating Systems and hardware, the method in which these are patched will be reevaluated to prevent downtime of critical infrastructure and to make those dependent on these machines more aware of the patching (Prowse, 2011, p. 148). The IT Security team will also be implementing various monitoring and assessment technology to prevent outbreaks of malware. This will be coupled with the effort to improve security of our internal devices by means of network vulnerability tests, social engineering tests, and stepping up the monitoring of security threat websites (Cobb, Cobb, & Kabay, 2009, pp. 15.19-20).

In order to maintain compliance with various federal regulations including SOX, GLBA, FISMA, and HIPAA, the security team also endeavors to create an incident response playbook. This playbook will serve as a go-to guide for the security team to document incidents that either have occurred or have the potential to occur as well as the procedures used to mitigate those risks (Miora, Kabay, & Cowens, 2009, p. 56.22). The proper use of the playbook will require the security team to test the procedures often and will likely be linked to various vulnerability tests and social engineering tests and may require input from members of different business organizations to complete but the value it produces will be of immeasurable value to improving the security of our customer data an intellectual property.

Conclusion

In conclusion, the various incidents that took place at Firion in the past year have provided a sincere and sobering look at the state of affairs within the company. Despite the challenges, the company has managed to survive some severe data breaches and will use the insight it has gained to improve security across the board. The majority of the instances where the company faced its greatest losses could have been prevented if there had been a change control system in place, proper data classification, an acceptable use policy, and enhanced security awareness. In light of these demands, the company has created proper tools to fill these gaps and should be able to prevent such losses in the future. With a special focus on the needs of its people to be part of its processes, Firion hopes to develop a culture that will be the envy of its competitors and it may accomplish just that.

Bibliography

What is sox – sarbanies oxley act. (2010). Retrieved from SOXResource: http://soxresource.com/what-is-sox/

Chinese Spies Use Fake Facebook Pages to Gain Intel. (2012, 3 12). Retrieved from Defensetech: Chinese Spies Use Fake Facebook Pages to Gain Intel

(2012). *Federal statutes.* Retrieved from http://it.ojp.gov/default.aspx?area=privacy&page=1285

Bamnote, G., Patil, G., & Shejole, A. (2010). Social Networking - Another Breach in the Wall. *International Conference on Methods and Models in Science and Technology*, 151-153.

Bamnote, G., Patil, G., & Shejole, A. (2010). Social Networking - Another Breach in the Wall. *International Conference on Methods and Models in Science and Technology*, 151-153.

Business Insider. (2011). *70 Million Playstation users had their credit information compromised*. Retrieved April 14, 2012, from Business Insider: Retrieved from http://www.businessinsider.com/imf-cyber-attacked-hackers-sony-rsa-lockheed-martin-epsilon-michaels-2011-6

Business Insider. (2011). *Email marketing firm Epsilon was hacked to obtain emails for 'spear phishing'*. Retrieved April 14, 2012, from Business Insider: http://www.businessinsider.com/imf-cyber-attacked-hackers-sony-rsa-lockheed-martin-epsilon-michaels-2011-6

Business Insider. (2011). *Google Announced*. Retrieved April 14, 2012, from Business Insider: Retrieved from http://www.businessinsider.com/imf-cyber-attacked-hackers-sony-rsa-lockheed-martin-epsilon-michaels-2011-

Cobb, C., Cobb, S., & Kabay, M. E. (2009). Penetrating Computer Systems and Networks. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol. 1* (pp. 15.1-15.36). Hoboken: John Wiley and Sons Publishing, Inc.

Donston, D. (2008, 5 19). WEB 2.0. *Eweek, 25(16), 25*(16), p. 39.

Goodrich, M. T., & Tamassia, R. (2011). *Introduction to Computer Security*. Boston: Pearson Education.

Goodrich, M. T., & Tamassia, R. (2011). *Introduction to Computer Security*. Boston: Pearson Education.

H. M. P. S. , H., & Wijayanayake, W. (2009). Computer misuse in the workplace. *Journal Of Business Continuity & Emergency Planning., 3*(3), 259-270.

Kabay, M. E., & Robertson, B. (2009). Security Policy Guidelines. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol 2* (pp. 44.1-44.17). Hoboken: John Wiley and Sons Publishing Inc.

Kabay, M. E., & Takacs, N. (2009). E-Mail and Internet Use Policies. In S. Boswrth, M. E. Kabay, & E. Whyne, *Computer Security Handbook Vol.2* (pp. 48.1-48.46). Hoboken: John Wiley and Sons Publishing Inc.

Kopp, E. (2008, 11 3). *Data Classification: A Cornerstone of Information Security*. Retrieved from NYSTEC.com: http://nystec.com/news_and_events/article_data_classification_a_cornerstone_of_information_security/

McEntegart, J. (2011, June 29). *Sony sued for negligence over ps3 hack.* Retrieved April 12, 2012, from Toms Guides: http://www.tomsguide.com/us/PSN-Hack-Lawsuit-Negligence-Breach-of-Contract-Privacy,news-11662.html

Miora, M. (2009). Disaster Recovery. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol. 2* (pp. 59.1-59.21). Hoboken: John Wiley and Sons Publishing Inc.

Miora, M., Kabay, M. E., & Cowens, B. (2009). Computer Security Incident Response Teams. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol. 2* (pp. 56.1-56.37). Hoboken: John Wiley and Sons Publishing, Inc.

(n.d.). *Summary of the HIPAA privacy rule*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

NIST. (2010). *Detailed overview.* NIST. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/overview.html

Prowse, D. L. (2011). *CompTIA Security+ SYO-201 Cert Guide*. Indianapolis: Pearson Education.

Raman, K., Baumes, S., Beets, K., & Ness, C. (2009). Social Engineering and Low-Tech Attacks. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol. 1* (pp. 19.1-19.22). Hoboken: John Wiley and Sons Publishing, Inc.

Reckard, E., & Menn , J. (2008, 8 2). Insider stole Countrywide applicants' data, FBI alleges. *Los Angeles Times*.

Rouse, M. (2011, 3 22). *Digital millennium copyright act (DMCA).* Retrieved from TechTarget.com: http://whatis.techtarget.com/definition/0,,sid9_gci904632,00.html

Rudolph, K. (2009). Implementing a Security Awareness Program. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol. 2* (pp. 49.1-49.43). Hoboken: John Wiley and Sons Publishing Inc.

Ruighaver, A., Maynard, S., & Warren, M. (2010, 10). Ethical decision making: Improving the quality of acceptable use policies. *Computer& Security, 29*(7), pp. 731-736. doi:10.1016/j.cose.2010.05.004

Sample Data Classification Policy. (n.d.). Retrieved from DataSecurityPolicies.com: http://www.datasecuritypolicies.com/sample-data-classification-policy/

Tittel, E. (2005). *PC Magazine Fighting Spyware, Viruses, and Malware.* Wiley Pub.

Verizon. (2011). *2011 Data Breach Investigations Report.*