Security Management

Steve Strickland
Steve Strickland Consulting
www.s3cc.net

Steve Strickland Consulting (S3CC IT Consulting) specializes in outsourced IT/Computer Consulting/Services. We specialize in the areas of managed IT & Computer Services (including repair), Network Security, Data Backup/Protection & Disaster Recovery, Document Management Solutions, Microsoft SharePoint Consulting, Hardware/Software sales, Computer Asset Management, Paperless Office Solutions, and Electronic Medical Records (EMR) Consulting. S3CC is a Certified Veteran-Owned Business and Certified Small Business.

All company names and dollar figures in this paper are fictitious and only used to illustrate the concepts of the actual paper. This paper was originally created for a school project and could be used a template for others or reading/education.

TABLE OF CONTENTS

Executive Summary

This paper will examine the performance of a risk assessment and then develop a risk management and maintenance plan to secure the computer and network systems from risks and threats. The rationale behind performing a risk assessment is due to the secure nature of the business where security is the most important issue and a high degree of security should be assumed since the organization develops network security software as a vendor. Additionally, the company holds patented and proprietary information, data, and software code on computers within the network.

In order to achieve this product, much research of the organization must be conducted. The purpose of the organization is to develop a top quality suite of software that is classified as network security and compliance software. The company holds several patents on the software code and design as well. Because the company is small, the network is relatively small in nature as well. Regardless of the size however, security is a top priority in the organization.

Researching the company will delve deep into the many aspects of risk assessment in order to develop a risk management and maintenance plan to ensure an even securer network and computer systems to thwart off risks and threats. When considering a risk assessment, security administration and controls should be taken into account. Additionally, the basic understanding of the fundamental principles of security should be discussed and analyzed as well. Throughout the paper as well, the organizational security model will be produced.

Organization Description

In security administration and controls, the three main sections are administrative controls, technical controls, and physical controls. Administrative controls define developing and publishing of policies and procedures, standards and guidelines, and risk management (Harris, 2008, p. 57). Technical controls, or logical controls, outline the implementing of access control mechanism (e.g. user access control), password policy and management, authentication methods, security devices, and configuration management (Harris, 2008, p. 57). The physical controls outline controlling access to certain areas of the facility and in different departments (e.g. server room), removable media policies, intrustion detection systems, and environmental controls (Harris, 2008, p. 57). Taking into account the security administration model, the physical controls encompass all other controls. The second layer of controls which sit right inside the physical is the technical controls. Inside the technical controls are the administrative controls. Lastly, residing deep in the security administration model is the company data and assets. Figure 1 outlines the layers.

Figure 1 - Security Administration Model

(Harris, 2008, p. 57)

The basic fundamental principles of security are outlined as availability, security objects, integrity (data and network), and confidentiality. Also, a corporate security policy can be included as well that discusses the principles of security. Figure 2 outlines the principles of security model.

Figure 2 - Security Principles Model (AIC Triad)

Availability is the top most object because without availability, none of the other objects would matter. If a server is not available because it is off the network and local connections are not available, the integrity and confidentiality is null because nobody can use the server in the first place. However, making the server and its data available and secure is the most important function simply because that data needs to be used at any time for anyone needing those

resources. Having a redundant system in place can increase availability as well, thus, reducing any single point of failure (Harris, 2008, p. 60).

Integrity is the assurance that data is clean, free from defect, available, non-corrupt, and reliable. This goes to say software and hardware should have a high degree of integrity as well. If you have a RAID card failing in the server periodically and causing outages, the integrity of that card is reduced and causes issues on the server and the overall network. However, discussing data integrity is also taking account security measures, such as user access controls, intrustion detection systems, and MD5 hashing. This will reduce an attacker's method of compromising data integrity.

Confidentiality comes down to the workforce themselves. Attackers come in all shapes and sizes and have numerous methods of attacking a network. Either through compromising a hole in the network from networking monitoring, shoulder surfing the unsuspecting users, stealing password files, or even social engineering. In an organization, excluding the network security, typical users should be trained to deter shoulder surfing, leaving passwords on paper or in files, and the effects of social engineering. A trained and alert employee that understands the breach of confidentially in the organization is an employee educated on basic security. The employee who is not trained and not alert is the prime target for a would-be hacker/attacker.

By developing security administration and controls, detailing the fundamental principles of security, and including a corporate security plan, a risk assessment will be completed, along with developing a risk management and maintenance plan.

Risk Assessment

In order to conduct a risk assessment, you must first establish the type of assessment. For example, an accounting risk assessment will be completely different from an Information Technology risk assessment. The purpose of a risk assessment is to identify mitigating risks, potential risks, asset management and valuation – and, if a threat or vulnerability is exposed and a disaster strikes, its potential on its affect on the organization as a whole, including departments, functions, and other processes as well.

According to the University of California Office of the President in the Information Resources and Communications department, the methodology of a risk assessment (RA) falls to nine guidelines. These guidelines include establishing the RA team. The team should consist of people from a wide range of departments in the organization that covers the entire organization. Scoping the project is critical because it lays down the foundation of the RA and defines the objectives, also including identifying all the members and stakeholders. Distinguishing assets is critical. Without some type of asset management system in place, an

organization will not be familiar with what they have, and will not be able to determine valuation of assets. Categorizing losses comes after establishing what you have and placing a value on that asset. If you value a computer at $3000 and that asset is damaged, it could cost $3000 to replace it. The identification of threats and vulnerabilities are left up to the security experts of the company, but need to be documented. Conducting an audit, one might find that Microsoft security updates are missing on several computers, potentially exposing them to attacks. One might also discover that the anti-virus software has not been updated in several months. Identifying the threats and vulnerabilities, and what tools and resources are used or needed to counter such should be part of the RA plan. This leads directly into identifying existing controls, which includes tools and resources. If the organization does not have a method of managing their assets, it would be in their best interest to conduct research and find a tool that addresses the need. After implementing the resource that will manage the risk, the threats, and vulnerabilities, then existing controls can safeguard the assets and data of the organization and it can be well protected. . Once all the data for the RA is collected, it should be analyzed to determine actual risks to assets. An example is having a server that faces the outside network and analyzing and determining the threats that can potentially happen to that sever. A server exposed to the outside network gives anyone with an Internet connection the ability to connect to that server. If that server is running a DBMS, even more threats can be exposed through the database and its application. Finally, reporting on the information collected, the determined assets, and the risk potential documentation should be prepared in a well-formatted report, and presented to management outside the RA team. In the event of a threat that may take place, or if a vulnerability has been exposed and damage to assets have occurred, including data which has taken place, not only does the disaster recovery program engage, but the risk assessment report can be used to determine the total assessment of damages (Risk Assessment Methodology Overview , 2008).

Asset Valuation

Intellectual Property (patents and copyrights)

In determining asset valuation of tangible and intangible property in the organization, the fair market value standard is used. Fair market value incorporates certain assumptions that estimate what a willing buyer would pay to a willing seller for most property. In retrospect, a value can be placed upon property, whether tangible or intangible. Intellectual property such as patents and copyrights come with price tags directed by the federal government. Patent prices from the United States Patent office as of October 02, 2008 cost $330 for filing and $540 for a searching fee (UNITED STATES PATENT AND TRADEMARK OFFICE FY 2009 FEE SCHEDULE, 2008). The organization in my project holds three patents on software design. Associating costs to patents is displayed in table 1.

Patent for:	Filing Fee	Searching Fee
Server-Side software design	$330.00	$540.00
Client-Side Software design	$330.00	$540.00
Console Application design	$330.00	$540.00
Totals	$990.00	$1620.00

Table 1 - Intellectual Property (Patents) Costs

Trade Secrets

Trade secrets come in the form of information that is generally not known to the public. Trade secrets are information, which is not generally known, or reasonably ascertainable, by which a business can obtain an economic advantage over competitors or customers (Wikiepedia - Trade Secret, 2008). At XYZ, trade secrets come in the form of our customer data. We collect and store customer contact information, remote access information, including usernames and passwords to computers where our software is installed. Other trade secrets we maintain are the non-public cost of our software and support services. Each customer is associated with a cost of how many licenses they have purchased, type of account they have (government, education, non-profit, or for-profit with respective prices), and what type of service they have purchased and its cost.

Associating a cost to customer data can include the pay-rate of the employee entering the data times the amount of time it takes to input such data. Additionally, cost of customer data can include the amount of revenue produced from that customer based on their purchase. Table 2 outlines sampling data, which is considered trade secrets.

Customer	Data Entry Time	Data Entry Cost	License Cost/year	Support Cost/year
Customer #1	30 minutes	$20	$10,000	$5,000
Customer #2	30 minutes	$20	$9,000	$5,000
Customer #3	30 minutes	$20	$12,000	$3,500
Customer #4	30 minutes	$20	$10,000	$5,000
Customer #5	30 minutes	$20	$6,000	$5,000
Totals	150 minutes	$100	$47,000	$23,500

Table 2 - Trade Secret Information and Cost Association

As table two outlines, XYZ, Inc. values the data entry cost at $100, license cost per year of $47,000, and support cost of $23,500 per year. Having costs associated with intangible items provides the baseline that in the event of a breach of security and trade secrets are stolen, it could initially cost the company $70,600 in damages.

Accounts Receivable

In reviewing the balance sheet of XYZ, Inc. (note: fictitious data is used), accounts receivable (AR) is noted, along with fixed asset costs. The AR is $336,973.30. Total fixed assets are $208,013.73. Fixed assets include furniture, tools and equipment, and automobiles. This brings total assets to $685,587.62 for the organization

ASI, Inc.
Balance Sheet

As of: 10/31/2008
Report Basis: Accrual

		As of 10/31/08
Assets		
Current Assets		
Cash		
	1005 - Undeposited Funds	14,646.80
	1010 - Checking	(21,029.66)
	1100 - Savings	150,102.31
Total Cash		**143,719.45**
Accounts Receivable		
	1200 - Accounts Receivable	336,973.30
Total Accounts Receivable		**336,973.30**
Other Current Assets		
	1230 - Owner Loan Receivable	(3,118.86)
Total Other Current Assets		**(3,118.86)**
Total Current Assets		**477,573.89**
Fixed Assets		
1400 - Fixed Assets		
	1415 - Furniture and Fixtures	12,000.00
	1420 - Tools & Equipment	156,556.00
	1435 - Vehicle	177,762.89
Total 1400 - Fixed Assets		**346,318.89**
1460 - Accumulated depreciation		
	1470 - A/D-Furniture and Fixtures	(4,800.00)
	1475 - A/D-Tools and Equipment	(62,400.00)
	1490 - A/D-Vehicle	(71,105.16)
Total 1460 - Accumulated depreciation		**(138,305.16)**
Total Fixed Assets		**208,013.73**
Total Assets		**685,587.62**

In terms of loosing AR and fixed assets, the economical downfall would be devastating to the organization. Not only would the company lose money due to downtime of equipment, the existence of threats can be quantified in a dollar amount in conjunction with downtime. If downtime is prolonged, accounts receivable comes to a standstill, thus, no money is generated during that time.

Physical assets all cost money and a value can be placed on every item. For example, a server would cost $3000. The database software that runs on that server costs $500. The time it takes the database administrator to install and configure the server and database is 6 hours and at a pay rate of $80 per hour, it would cost $480. A grand total cost for that single asset would be $3980.00. In the event of a security breach to the server and database, it could essentially cost the organization $3980.00 to replace/repair that server. At XYZ Inc., physical assets are listed in table 3 with associated costs.

Equipment	Cost	Software	Cost	Employee Hours	Employee Pay Rate	Total Cost of Asset
Server	$3000	Database	$500	6	$80	$3980
Server	$3000	Email	$1000	8	$80	$4640
Router	$2500	None	$0	3	$80	$2740
Firewall	$1000	None	$0	3	$80	$1240
Server	$3000	SAN	$2000	8	$80	$5640
Client Workstations	$1200 x 10 ($12,000)	Operating System + Client Software	$1000 x 10 ($10,000)	3 hours x 10 (30 hours)	$80	$24,400
Totals	$24,500		$13,500	58		$42,640

Table 3 - Trade Secret Information and Cost Association

By associating costs with physical assets, including the intangible cost of time * cost of time, we arrive at a total cost of that assets. If a breach of security takes place, the cost of repair can be quantified.

As the book notes, qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted with the goal of seeing how a business will be affected by different threats and losses, in terms of operational and economical (Harris, 2008, p. 781). Lose criteria should be associated with individual threats, keeping in mind the cost associated to tangible and non-tangible property. The lose criteria should include (Harris, 2008, p. 781):

- Loss in reputation and public confidence, which can result in lower sales, costing the company revenue.
- Loss of competitive advantages, resulting in losing the customer base to competitors.
- Increase in operational expense, possibly due to paying overtime wages, replacing hardware and software, and hiring outside personnel.
- Violations of contract agreements, with potential legal issues rising, causing more money to be spent.
- Violations of legal and regulatory requirements, resulting in fines from governing bodies and failed audits.
- Delayed income costs
- Loss in revenue (due to downtime, threats, and losing a customer base)
- Loss in productivity, due to employees now having to shift their focus from their daily activities to “cleaning up” the aftermath of an attack/breach.

Risk Assessment Method

The risk assessment method I have chosen for the project is the qualitative method. Qualitative risk management is widely known and used in businesses since qualitative risk analysis methodologies use a number of elements, such as threats, vulnerabilities, and controls (Introduction to Risk Analysis, 2003). These are elements that can be depicted and are simple to convert into a risk assessment that fits the company in this paper. Threats are possibilities that things can go wrong, whether assets are damaged internally or externally. Vulnerabilities include “holes” in the system that would expose that system and make it prone to attack from a virus or hacker, and increase the likelihood that an attack would be successful. Controls are mechanism in which are used to evade and counter threats and vulnerabilities, such as applying security patches issues by vendors, perimeter security, server and network security, and desktop security. Such devices might include proxy servers, firewalls, anti-virus/anti-spam/anti-spyware software. Prevention is the key to controls – to prevent the threat and reduce the vulnerability so they do not happen.

In a quantitative risk assessment analysis, assigning a dollar value, while conducting asset valuation, can be accomplished, but probability data must be used. All property, tangible, and non-tangible, can be translated into a value which the organization can use, mainly, a dollar figure, including time and material.

Quantitative risk assessment includes the calculation of the single loss expectancy (SLE) of an asset. The single loss expectancy could be defined as the loss of value to assets based on a single security incident (How to Develop a Risk Management Plan, 2008). The calculation is:

Single Loss Expectancy (SLE) = Asset Value (AV) x Exposure Factor (EF)

Exposure factor is a percentage of an asset loss. If an asset is half-lost, the EF would 0.5. If the asset if 100% lost, the EF would 1.0. Consider the following equation:

SLE = $3000 (AF of server) x 0.5 (EF and taking into account that only half the server could ever be destroyed due to certain redundancy built into the computer). $3000 x 0.5 = $1500. The SLE = $1500.

Including the SLE of assets is part of the quantitative risk assessment.

Risk Management Strategies

In this paper, risk management refers to planning for adverse events (disasters) that can impact an organization, particularly in a financial way. Risk is the effect (positive or negative) of an event, computed from the probability of the event materializing (becoming an issue) and the impact it would have (Risk = Probability x Impact) (How to Develop a Risk Management Plan, 2008).

To assess risk, many factors must be taken into account which includes the event itself, the probability of that event happening, the impact if that event happens, and mitigation risk countermeasures (prevention), or contingency.

In my organization, the following risk matrix outlines events, and risk assessment:

Event	Possibility (which takes into account the event running 24x7x365 with zero issues)	Impact	Countermeasure	Contingency Plan
Email Server non-operational	10%	All email in the organization will be non-operational except inter-office	Establish security policy which includes SMTP server behind firewall,	Establish secondary fail-over MX records. If the main MX routing

		email.	no relaying, and anti-spam controls in place	is non-operational, the secondary takes over.
Domain controller non-operational	10%	Users of that domain would be unable to log in and access network resources	Operational controls need to be in effect to monitor server services and health, alerting administrators of out of norm status.	Secondary domain controller would be in place and rolled over into main domain, if the main domain were to fail.
Internet outage	20%	All inbound/outbound traffic would cease immediately. Email would not be routed. E-Commerce would be affected, the website would be offline.	Establish SLA with provider to guarantee uptime. Have readily information for technical support from provider.	Establish dial-up plan with provider in the event that the high-speed connection goes offline. A dial-up connection will bring the Internet connection operational.
Router non-operational	10%	All DNS and DHCP activity would cease. All inbound/outbound traffic would be halted.	Establish firewall policies, VPN policies, and operational controls need to be in effect.	Having a secondary router in place that will become an alternative hop in the routing if the main router fails.
Theft (physical	1%	Depending on the equipment stolen,	Establish security policies	Operational controls would

equipment)		the impact would pertain to that equipment and its operation.	and security awareness training. Operational controls would include physical deterrence to certain equipment (i.e. IT personnel only allowed in server room)	need to be in effect. Security policies would need to be enforced and adhered to. Security awareness training would need to be accomplished.
Theft (breach, hack, stolen/destroyed data)	10%	Company or department-wide operations could be halted. Illegal activities could mitigate. Financial hardship could take place.	Enforcing security policies and security awareness training. Having proper security in place (updated security patches, anti-virus, anti-spyware, anti-malware, firewall policies)	Having the proper incident response team and tools established and trained. Having proper backup plans and a full disaster recovery plan in effect.

Table 4 - Risk Matrix

Assignment of Risks

Risks should be assigned so they fall into categories of most important to least important. While all risks should be regarded as crucial, they must be assigned a probability label and an impact label. To assign probabilities of the risk becoming an event, the following tables prioritize different levels of risk:

Probability of this risk to happen		
H	High Risk	This event has happened frequently and the possibility of this event happening again is extremely high.
M	Medium	This event happens occasionally and the possibility of happening again is reasonable to expect it to happen again at least once in the next year.
L	Low	This event rarely happens and in the past year, it has only happened once.

Table 5 - Probability Table

Impact if this risk becomes an issue		
H	High	A highly visible event and will have a major impact on the organization, its operations, and could include financial issues.
M	Medium	This will cause disruptions with users, data flow, and operations, but will not be highly visible.
L	Low	This will cause minor disruptions in operations/services and will have minimal impact on the organization.

Table 6 - Impact Table

Risks that fall into the HIGH category will have the largest impact; thus, will be the most scrutinized and observed. Risks deemed LOW will be less watched and usually a single person or small team will be assigned to monitor them.

The following table outlines the risk, probability rating, and impact rating:

Risk	Probability Rating	Impact Rating
Email Server non-operational	L	H
Domain controller non-operational	L	M
Internet outage	L	M
Router non-operational	L	M
Theft (physical equipment)	M	H
Theft (breach, hack, stolen/destroyed data)	M	H

Table 7 - Probability/Impact Rating

Countermeasures

A countermeasure is an action, process, device, or system that can prevent, or mitigate, the effects of threats (Defintion - Countermeasure, 2006) - and in this project, threats to the organizational technology and data. Countermeasures come in all shapes and sizes from knowledge, security policies, security awareness, software, and hardware.

When planning for countermeasures, a certain degree of planning comes into focus. Knowing all the risks in the organization is a start. Knowing the equipment and data is another step. Knowing the impact of an event happening from a breached risk is yet another step in the entire process of planning for countermeasures. Planning for counter measures also includes natural and/or human-caused risks (earthquake or employee X drops his computer down a flight of stairs when moving to a new floor). Everyone is faced with “what if” situations in a negative way. Planning for that “what if” event is critical to thwarting off the event before it can happen to reduce the risk (I should have a firewall operational before I let my users start browsing the Internet), or, in the event it does happen, steps can be taken to counter the issue (anti-virus software installed, updated, and enabled so when a virus arrives, it can be stopped immediately).

Planning should always include preventive measures and “after the fact” measures. Preventive measures would include knowledge transfers for incoming/outgoing employees, enforced security policies, security awareness training, proper software in place, which can include anti-virus, anti-spyware, anti-malware, and proper hardware in place, including firewalls, and ACL lists on routers, network access controls, proxy servers, and strategic backup plans. Post-measures can include incident response teams and management teams who are fully trained on disaster recovery plans.

Incident handling policies

Computer security incident management requires computer security and information technology in terms of monitoring, detecting, and responding to events that take place on computers, the network, and their information. An example would be employee A is caught sending harassing email to another employee, corporate documents are stolen from a USB memory stick that employee B had with sensitive corporate documents, or there was a security breach into the network from a hacker. Incidents can usually range in categories such as normal, escalated, and emergency. Incident teams are usually trained in all aspects of what could be classified as an incident, including network security and the comprehensive corporate policy.

According to the International Organization for Standardization (ISO), they publish ISO/IEC 27002 (ISO27k), which is an information security standard of code used for the practice of information security management outlined in Section 9. In incident handling policies, and according to the ISO 20072 guidelines (Incident Management Guidelines), there are five main stages to be considered in an incident handling process:

1. Containment
2. Assessment
3. Countermeasures
4. Appraisal
5. Conclusion

However, before moving into the five categories, the incident must be qualified, and be determined whether or not the event even qualifies as an incident. Questions such as has there been a treat to the company’s business assets, a breach of security or corporate security policy. While an organization should use their best judgment on how to proceed with each of the handling processes, a policy should be in place for when events do take place. Response and readiness teams should be qualified and trained and policies enforced from the CEO level down.

Business Continuity

Change Controls and Disaster Recovery

Change controls, like disaster recovery procedures, have categories. In an article by George Spafford, he outlines the change control categories as prevent, detective, and corrective (Spafford, 2003).

In the preventive category, the control is prevention of unauthorized changes. The help desk technician would not be allowed to make database changes relating to security. Network access controls in place enforce the prevention. Processes of a change management plan are utilized. The detective category is detecting and identifying unauthorized changes. If security is changed on a database server and nobody knows about it and the risk level is now elevated, an event like this needs to be detected. If financial data is being accessed by non-authorized personnel, an event like this needs to be detected. However, in the preventive category, administration can hope incidents like this do not happen without a proper change management policy in effect. Unauthorized changes and access should be prevented, and in the case of them not being prevented, mechanisms should be in place to detect, identify, and notify. In the corrective category, when unauthorized changes are made, corrective steps should be outlined to bring operations back to the state they were in before the change. Using backups is a perfect example along with using software that records activities so it can be easily reversed is another example.

In disaster recovery, a full plan is utilized and many “what if” situations have solutions. Disaster recovery, which is sometimes referred to as business continuity planning (BCP), has evolved from the simple backups performed on servers and databases (although most still only do that). It has evolved into a full process implemented into an entire organization complete with policies and procedures that restore operations critical to business operations, including access to data, software, hardware, communications, and business processes. However, organizations can still have disaster recovery plans inside a huge BCP as well, say, disaster recovery on a division or department basis. With a solid BCP that involves disaster recovery, recovery point objectives and recovery time objectives should therefore be established. Additionally, contingency plans, maintenance, implementation, and planned staged disaster recovery drills should be discussed, designed, and included in the BCP.

The basics of disaster recover should be backing up data – especially critical data that pertain to the operations of the organization. Identifying preventive controls should play a key role. According to the National Institute of Standards and Technology, who write BCP’s for the federal government, identifying preventive controls can save time, energy, money, resources and a lot of headaches down the road. Their policy on common measures are using

appropriately sized UPS to provide short-term backup power, gas powered generators for long-term backup power, proper air conditioning and ventilation , fire suppression systems, fire and smoke alarms, water sensor in the computer room ceiling and floor, plastic tarps to drape over equipment in case of water disaster, emergency master system shutdown switch, offsite store of backup media, technical security controls, and frequent, scheduled backups (Contingency Planning Guide for Information Technology Systems, 2002).

The relationship between change controls and disaster recovery are close to each other. In one aspect, change controls help to prevent and document, while disaster recovery is recovery after the fact. However, with both of them working side by side, they create the bubble around the organization that provides an overall secure and protected nature for services, data, software, and hardware.

Tools of the Trade

Electronic email is probably the most widely used form of electronic communication for any organization. Email is also highly vulnerable to an organization if unprotected, not included in corporate security policies, and exposed to disasters from attacks or loss of data which can leave an organization in chaos. Email attacks can come in the form of viruses attached to emails, phishing emails tricking the unknowingly user into giving away data, including usernames and password, and spyware and malware, that can be just as destructive as viruses. Viruses, spyware and malware all share in the same nature of being able to destroy data, turning your computer into a zombie or hijacking your computer, and causing risks to be elevated enough to cause severe problems in the organization, technologically, and financially.

Tools – software and hardware - are the part of the best defense IT staff can use to reduce or possibly eliminate risks. Software tools would include anti-virus and anti-spyware applications (which most AV software now comes bundled with anti-spyware and anti-malware), and also anti-spam tools (at the email client and server level). Anti-spam software is beneficial in the way that it can include anti-virus protection, so while filtering out unwanted emails; it will scan all emails and attachments for viruses. Symantec Corporation offers a wide variety of tools for protecting email. Their complete anti-virus suite not only protects at the desktop level, but can be implemented into a variety of email servers to add protection to all email. Symantec offers Brightmail message filtering as well for the control and management of unwanted email. GFI Corporation developers GFI Mail Essentials software that incorporates into the email server so provide total control over email protection, including anti-virus, anti-spam, anti-spyware, and anti-malware. Other companies, such as McAfee and Trend Micro offer email protection solutions as well. For companies that do not host their own email, their hosting company will usually provide email protection on their end. However, desktop level software, such as

Symantec Corporate Anti-virus or Microsoft Forefront Client Security can provide that suite of anti- virus/spyware/malware/spam application.

Disaster Recovery Options

In the organization for this project, the disaster recovery options are limited, but vital. Daily backup schedules are in place for critical servers, which are the email server, and small business server which acts as a primary domain controller, DNS server, printer server, and file server. Select computers are backed up weekly as well. The Internet connection from the hosting company comes with a solid SLA to provide maximum uptime, including a two hour turnaround time in the case of an outage. Due to the strong SLA from the hosting company, redundancy is not built into the Internet connection. A two-hour downtime is a small window, thus, reducing the risk.

Other disaster recovery options include a secondary router on standby mode. The ease of having a second router operational is a matter of moving a few CAT5 cables, inputting the IP address, subnet make, gateway address, and DNS addresses from the hosting company, and the secondary router would be operational.

Other disaster recovery options come with preventive measures in place. All computers, including servers, have anti-virus software. All computers, including servers, are checked monthly for security updates that are issues by various vendors. Desktop computers have message filtering client software to work with their email client software, including anti-spyware, and anti-malware protection. The email server provides anti-spam filtering and control. All desktop computers use personal firewall software, while the perimeter of the network resides the main firewall.

Above all though, there is a disaster recovery plan and trained incident response team in place in the event an incident takes place. Procedures and documentation take place, along with salvage and recovery modes.

Roles and Responsibilities

A simple matrix outline roles and responsibilities pertain to the business continuity of the organization. They range from a disaster recovery team, incident response team, to stakeholders.

Member	Disaster Recovery	Incident Response	Stakeholder
Tony			X
Steve	X	X	X
Max	X	X	X
Mark	X	X	X

Table 8 - Roles and Responsibilities

Termination Procedures

With a person that is in a non-management or non-executive position, sometimes, the surprise termination is the best method. Upper management approaches the employee – states they are being terminated, security personnel (if needed or on staff) (or someone with authority) stays with the employee while they gather their personal items, and is escorted. This gives the now ex-employee no time to cause any damage, technically or physically, to anything.

After that usually uncomfortable situation is complete, an audit should take place. Using a simple checklist can usually accomplish a quick and simple audit, following (How to terminate network administrator's employment?, 2007):

- Change the local password on the employee computer
- Change their administrator password or disable their account all together
- Depending on their job, change any administrative password that the employee knew of or had access to (databases, file servers, email servers, etc).
- Change their email password
- Disable any remote access the employee had, including telnet, http, VPN, and FTP access.
- Secure all physical property the employee had, such as rack server keys, key access cards, etc.

- Over time, auditing of log files can be examined to determine if the ex-employee was doing anything before termination, and attempting to do anything post-termination.
- Inform personnel. In one such case, an employee was terminated, but nobody was informed. The ex-employee came back the next day acting as if he was not terminated (subtly escaping the people that fired him), and complained to the security admin “hey man, my password doesn’t work, can you reset it for me?” and he’s back on the network (probably to cause damage).

As the book notes, separation of duties should be performed in the organization. The object of separation of duties is to ensure that one person acting alone cannot compromise the company’s security in any way (Harris, 2008, p. 1029). While this plays into administrative management, it can also help in the long run when an employee is terminated. If the network administrator is terminated, you can be assured that whatever they were doing before or after termination and an audit is conducted, it will not involve diving into functions or tasks that pertain to the help desk, or to the security administrator. In the end, it will save time and vital documentation can be processed. Keeping record of who is who and who does what and has access to what – including what will be and what was changed pre- and post-termination, will provide an added layer of security and peace of mind.

Physical Security

Physical security involves data marking, as well as physical security of assets.

Data marking comes in different forms, and sometimes, can be up to an individual or organization on how they classify their data and its physical handling. The federal government for example uses three classifications: Top Secret, Secret, and Confidential (Marking Classified National Security Information, 2007). The organization can use any method of marking data – as long as employees know the meanings and their boundaries. The worker in the mail room is not allowed to review Top Secret marked data, but the CEO has access.

Data that is deemed to be categorized should be handled properly. It’s being marked for a reason. A document welcoming new hires probably would not be marked, but a document discussing executive pay rates will be marked. Polices should be put in place for such marked data as well.

Employees of certain levels can view certain types of data. As long as employees know their boundaries and understand the meanings of the markings, and proper corporate security policies are in effect, the electronics and physical security measures of data can be properly handled. A well-versed security officer will have plans in effect to control the flow of data,

monitor who has access to what systems that access such data, and what goes on with that data. Physical security is a must as well since some documents can be printed, even though limited to certain personnel. Some data should never reside on a laptop or mobile device and never leave the organization.
Establishing a business continuity plan, having an incident response plan and team (and trained), and disaster recovery plan all attribute to the proper handling of sensitive data in the organization. The Internet2 organization produces a blueprint on confidential data handling, and they outline as follows (Confidential Data Handling Blueprint, 2008):

- Create a security risk-aware culture that includes an information security risk management program
- Define institutional data types (marking)
- Clarify responsibilities and accountability for safeguarding confidential/sensitive data
- Reduce access to confidential/sensitive data not absolutely essential to institutional processes
- Establish and implement stricter controls for safeguarding confidential/sensitive data
- Provide awareness and training
- Verify compliance routinely with your policies and procedures

Having the key components of “how to…” will ultimately lead to safety, education, damage control, anti-theft, and highly secure and proper data handling.

Other physical security measures pertain to physical security of the organization and assets. Employees use a key-card to enter the building. Employees use a key-card to enter the serve room. All assets are tagged with asset tags and recorded. Employees having laptops, company cell phones or PDA devices sign documents about the role and responsibility of using company assets. All employees, when hired, sign documents pertaining to the safeguard of company assets and become more familiar with procedures during security awareness training.

To increase security in the workplace, safeguards are necessary and must be in place. As stated, entrance into the server room is restricted to key personnel only, and a key-card must be used. Information such as which the employee entered, time and date are recorded. Security cameras are in effect on the site to prevent asset theft. In terms of network security, a corporate security policy is established. Physical assets on the network provide the security needed – such as firewalls and proxy servers.

Risk Management

Risk management can mean many things to an organization, but above all, it is managing any and all risks that can have a detrimental effect to the organization, its operations, processes, finances, assets, and personnel. By creating a risk management plan, the organization can become better equipped and prepared to manage risks. As stated in Murphy's Law, "if anything can go wrong, it will." In any organization conducting some type of business activities, there will always be at least one thing that can go wrong, and in all likelihood, it will evolve from a risk on paper to an event that requires intervention and resolution. Risk management provides the tools, guides, and knowledge to mitigate risks, and to promote an even flowing activities of business with minimal or no disruption.

Legal and Ethical Considerations

In a typical organization, there are policies and procedures in place for information security, data handling, disaster recover, and a wide range of other duties pertaining to information technology overall. Additionally, in any organization, a certain degree of confidential data will be presently.

Whether that information is as simple as a mailing listing consisting of a customer's name and address, or much broader as to having customers social security numbers, credit card numbers, or even confidential medical, military, or government data could be stored somewhere on a computer system in that organization. In any event, legal, regulatory, and ethical considerations and requirements come into play to amount to stringent protection of that data in which IT security professional maintain and preserve.

Legal and ethical considerations arise in my organization to the type of data stored in conjunction with business activities. Types of data we collect and store are customer names, organization, addresses, and credit card information. This type of data is stored on paper and in databases, and with that, physical security and information security come into play in the organization.

When such confidential information enters the organization, not only do security safeguards need to be in place to protect such data, but legal and ethical considers are also in place. Legally, the organization cannot misuse the customer credit card for anything other than what the customer has authorized to be charged. In this case, it would be monthly fees for licensing of software and services. Other legal considerations are placed upon the organization for the software being produced. Software faults and protection come into account. Through a license agreement, the user must accept it before installing our software. If the user refuses the agreement, they should not install the software. However, that does not release the vendor of the software from legal issues. Legal issues my chosen

organization takes into consideration are trade practices to comply with export laws, reasonable foreseeable loss and damage to information systems assets that could be caused by the software, fully disclosing any bugs in the software that could be destructive to data, including logging such information, and transmission of data outside the customers network.

Ethical considerations the organization takes into account are who should have access to what data, who is responsible for maintaining accuracy and security, who is responsible when data is compromised, does the information's availability justify its use, and should employees know about security measures in place and how much of their activity is being monitored, especially for legal issues (Five ethical dilemmas IT leaders must confront, 2008).

Who has access to what data is an important decision. Establishing a business continuity plan, having an incident response plan and team (and trained), and disaster recovery plan all attribute to the proper handling of sensitive data in the organization. The Internet2 organization produces a blueprint on confidential data handling, and they outline as follows (Confidential Data Handling Blueprint, 2008):

- Create a security risk-aware culture that includes an information security risk management program
- Define institutional data types (marking)
- Clarify responsibilities and accountability for safeguarding confidential/sensitive data
- Reduce access to confidential/sensitive data not absolutely essential to institutional processes
- Establish and implement stricter controls for safeguarding confidential/sensitive data
- Provide awareness and training
- Verify compliance routinely with your policies and procedures

Having the key components of "how to…" will ultimately lead to safety, education, damage control, anti-theft, and highly secure and proper data handling.

Personnel who are responsible for the security of the data falls in-line with information security specialist, incident response teams, and information technology executives. A good security officer will have plans in effect to control the flow of data, who has access to what systems that access what data, and what goes on with that data. Physical security is a must as well. Some documents can be printed, but only by certain personnel. Some data should never reside on a laptop or mobile device and never leave the organization.

Responsibility comes in all shapes and sizes, but most importantly, the organization should know who is ultimately responsible when data is compromised. Is it the CEO or the database security specialist when a database is compromised and data is stolen? In my chosen organization, the responsibility would fall upon the CEO and CTO. Any organization should have a team of who is responsible when a data breach occurs and how to handle the aftermath.

Information's availability can conjure many ethical issues. Just because employee X in accounting has access to payroll records does not mean they should be emailing such information to employee B inquiring about unused paid time off or their wage information. Internal email can be monitored by IT staff, thus, letting IT staff know accounting information about employee B. Simply because information is available does not give free range to whoever accesses it. Using responsibility, common sense, and complying with company policies and procedures encompasses any ethical issues an employee or company would have considering the availability of information.

Lastly, informing employees about company owned information and assets and how much the employee should know is solely up to the organization. In my chosen organization, all employees sign an employment agreement. In such agreement, reference to the corporate security policy is made aware, and that information and activity monitoring does take place, for example, email monitoring. Email monitoring is done for legal issues to ensure that private data is not used improperly.

Current Legal and Regulatory Issues

While my chosen organization is not a publically traded or funded company, we do not fall under any regulatory issues. However, legal issues we do. Since the organization accepts confidential information from customers (credit card data for example), we fall under consumer protection laws and Payment Card Industry (PCI) security standards governing the use, misuse, and protection of credit cards. To become PCI compliant, the organization undergoes an audit of security measures, which are outlined by the PCI Security Standards Council. These audits include penetration testing, application firewalls, PCI security audit procedures, security scanning procedures, technical and operations requirements, and validation requirements. All of these audits ensure that the organization will use information properly and secure information properly using proper procedures, guidelines, and information security.

Impact of Security Controls

In security administration and controls, the three main sections are administrative controls, technical controls, and physical controls. Administrative controls define developing and publishing of policies and procedures, standards and guidelines, and risk management

(Harris, 2008, p. 57). Technical controls, or logical controls, outline the implementing of access control mechanism (e.g. user access control), password policy and management, authentication methods, security devices, and configuration management (Harris, 2008, p. 57). The physical controls outline controlling access to certain areas of the facility and in different departments (e.g. server room), removable media policies, intrustion detection systems, and environmental controls (Harris, 2008, p. 57). Taking into account the security administration model, the physical controls encompass all other controls. The second layer of controls which sit right inside the physical is the technical controls. Inside the technical controls are the administrative controls. Lastly, residing deep in the security administration model is the company data and assets.

The overall impact of these controls on personal privacy of system users is minimal. For example, while information monitoring is conducted, it is not conducted with every single activity users do. The personal privacy of users is respected, however, through monitoring and security controls, users forfeit certain privacy rights in the organization. For example, users are cautioned on personal email conducted through company email. From the corporate security policy in effect, users are aware that information stored on their computer is company property and will be monitored and used as the company sees fit. In another example, employees are prohibited from storing personal photos (i.e. the family vacation) on company computer systems. Users are aware that such data will be removed if the user does not comply with the corporate security policy.

Strategies

Due to the organization storing and processing credit card information and confidential information and falling under PCI regulatory compliance, strategies take place to keep the organization in compliance. Additionally, the organization works with other organizations that process credit card information who are not PCI compliant and we work with them to bring them to full compliance.

One strategy the organization engages in is having the information technology staff (full time and contractor) becomes certified from the PCI Security Standard Council. The organization and staff go through training and audits to become a qualified security assessor (QSA) and approved scanning vendor (ASV). Employees becoming qualified security assessors must meet requirements set forth by the PCI Security Standards Council, such as have sufficient information security knowledge and experience to conduct technically complex security assessments, process industry-recognized security certification(s) or equivalent work experience, be knowledgably about the PCI DSS and the PCI DSS Security Audit procedures, attend annual training provided by the PCI SSC, and be employed by a Qualified Service assessor organization.

Since the organization is QSA approved and key employees are ASV, the organization not only complies fully with PCI security standards, but improvise security with other vendors and cliental to being them to PCI compliance standards as well.

The Law and Ethics

In any given organization; public or private; legal, regulatory, and ethical considerations takes place daily in any routing business operations. Whether the company is dealing with electronic data, physical assets, or even paper based data, security is always a concern to an organization. Knowing how to secure that data and employing proper handling techniques, whether through simple policies and procedures or strict requirements from governing regulations, such as SOX or HIPAA, the organization can ensure that they are practicing within the law and have placed the highest standards of ethics upon their data, their clients, and the organization itself.

Maintenance Plan Policies

In any given organization, data exist in one form or another. That data revolves around a structure to ensuring security, integrity, access controls, and availability. Within this structure, policies and procedures are established to ensure all the above mentioned function properly. Without policies and procedures, security risks are increased to the data, users, and the organization, and thus, security management and maintenance plans are developed. A full security management plan involves many concepts that encompass the security of the entire organization. Within the security management plan is a maintenance plan. The maintenance plan would include policies, procedures, standards, guidelines, change management, and hardware/software lifecycles.

With a security maintenance plan, the International Organization for Standardization outlines the ISO/IEC 17799:2005 publication on information security. The ISO 17799 outlines general categories and practices in the areas of information security that are part of a maintenance plan, such as:

- Security policies
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management

- Business continuity management
- Compliance

(ISO/IEC 17799:2005 Information technology)

Security policies can mean a range of things in various organizations. If the company falls into governing regulations, they must comply with some compliancy, such as SOX, HIPAA, GLB, ISO, or PCI. While other organizations might not fall under those compliances and would outline pre-defined policies, these organizations conclude to other policies they invent for the specifics of the organization, or borrow from governing compliances or other standards.

In most organizations, they will have some type of corporate security policy plan. Corporate security policies would define and detail such items as acceptable usage, remote access controls, email usage, password policies, firewall policies, and wireless security policies. Policies involved in security of information technology to the organization exist to identify assets that the organization deems valuable, provides authority to security teams, provides a reference to review when conflicts pertaining to security arise, states the organization's goal and objectives pertaining to security, outlines personnel responsibility, helps to prevent unaccounted-for events, defines the scope of the security teams, outlines incident response responsibilities, and outlines the company's response to legal, regulatory, and standards of due care (Harris, 2008, p. 111).

Procedures

Procedures entail the "how to" guidelines that organizations follow. These how to steps apply to IT staff, operations staff, security members, and others who deal with information technology. Procedures spell out how the policy, standards, and guidelines will actually be implemented in an operating environment (Harris, 2008, p. 115). An example would be how backups are performed noting who the team members area, what is backed up, when such data is backed up, and storage and security of the backup. Procedures should provide enough detailed information that is understandable to not just information technology personnel, but to a wide range of personnel (for example, CTO) (Harris, 2008, p. 115). The University of Illinois' National Center for Supercomputing Applications (NCSA) provides national standards on security policies and procedures. The sub-section relating to procedures outlines:

- Establishing policies and procedures
- Incident reporting
- Security implementation plans
- Project security procedures

- Publication and Presentation
- Copyright and Releases
- Newsletters and Public Information and Technical Materials

(NCSA Security Policies and Procedures, 2005)

This set of standards can guide an organization to producing meaningful, detailed procedures that incorporate security to meet the goals of the organization.

Standards and Guidelines

Standards and guidelines can fall into many categories which would include an information technology security program framework, business impact and vulnerability assessments, threat and risk analysis, personnel security standards, physical security standards, data security, network security, and access control security. Depending on how the organization operates will ultimately outline their standards and guidelines.

In my chosen organization we employ all the standards and guidelines discussed here. Personnel security is conducted through a corporate security policy. Physical security standards and guidelines are defined to protect network equipment and company assets. Data security standards are outlined with access control policies and content management. Network security is detailed with standards and guidelines in the corporate security policy

Change Management

Change Management is an IT Service Management discipline. The objective of Change Management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled IT infrastructure, in order to minimize the number and impact of any related incidents upon service (Change Management (ITSM), 2008). IT Service Management falls under the Information Technology Infrastructure Library (ITIL) which is a published series of practices with comprehensive checklists, task, and procedures that can be utilized by any IT organization.

In my chosen organization, change management exists, but only to a certain degree. Since change management here is used to ensure methods and procedures are used to efficient and prompt handling of all changes to the IT infrastructure, there are procedures the IT department follow when making changes. The IT department, following procedures, is responsible for hardware, communications equipment and software, system/network software, and all documentation pertaining to technology of the organization and the software that is designed by the company. Where change is needed, IT personnel submit their changes and requests though a chain of either the Director of Software Development or Chief software developer and/or the Director of Information Technology and Services. Once approved, the IT

staff will carry out the change. If need be, non-IT staff will be notified of any changes that could affect them and their services.

Hardware and Software Lifecycles

Hardware and software lifecycles outline the time frame of when to replace hardware and software. Most organizations subscribe to the 3-year or 4-year plan since newer and improved technology is released into the market place on that cycle as well. Depending on budgets and costs, some companies might go as low as a 2-year cycle, while others might go on a 5 or 6-year cycle. Microsoft Windows XP, as an example, was released in 2001. Today, in 2008, and most organizations still using Windows XP, are stretching into a 7-year cycle. Lifecycles are particular to the organization. An organization might underestimate the power needed in a server due to growth and might replace the older server, which could possibly be only two years old, or they can add an additional server. In all cases, the lifecycle will be unique to the organization and what hardware and software they are using and how they are using it.

Considerations must be taken into account as well. Outdated hardware systems can be vulnerable to attacks. Security fixes and vulnerability patches are often not supported on older systems. Older systems lose their warranties from vendors, thus, becoming more expensive to maintain from hardware failures. Lifecycle planning in an organization can come from different angles such as capital expense budgets (budget planning), warranty expiration, or waiting until the equipment fails (Computer Life Cycle Management and Migration, 2008). In all cases, planning for migration is an important step whether you are simply replacing anti-virus software, a simple and quick replacement, or if you are replacing a highly available database server, which takes planning for migration needs and must follow procedures to ensure data integrity remains intact and services are not disrupted, and of course, that the new hardware will be fully supported.

In my chosen organization, the hardware goes on a 4-year lifecycle and software goes on a cycle of 4 to 5-year lifecycles (excluding operating systems). When replacing hardware, a planning or migration and disaster recovery take place before new hardware is introduced. Depending on software, it is usually introduced through planning and migration or simply removing old software and installing new software.

Awareness Training

While my organization provides no formal security awareness training that is lengthy and detailed, we do provide a small amount of awareness training to all employees. The awareness training involves access control from data classifications, physical security, anti-theft, portable devices and laptop security, wireless security, e-mail security, and common

sense scenarios. The security awareness training focuses on and explains proper rules of behavior for the use of systems and information, expectations of users, and sanctions imposed for noncompliance.

Special attention is made to portable device and laptop security, along with e-mail security. Almost everyone in the organization uses laptops and portable devices. While they mostly do not carry classified or secure information on their computers, there is a chance they could carry low security documents at one point. Being aware of the security involved that is placed on not just the physical device from theft, but theft of data helps guide the user from right and wrong. The awareness provides the users the mechanism to understand security as it relates to the organization and its operations and that everyone has a different role in ensuring security is not compromised.

Identify areas within your organization where special attention should be paid to providing awareness training.

Maintenance Implementation Plan

A maintenance implementation plan in my organization would entail implementing the corporate security policy step by step. Since the corporate security policy encompasses all security for the organization – some parts of the plan relating to personnel, while other parts relating to assets, each section needs to implemented in a different manner. Parts of the plan relating to personnel are implemented during security awareness training, for example. However, disaster recovery and the teams responsible implement DR in a completely different manner. Since the organization falls under the Payment Card Industry (PCI) standards, implementing maintenance and security to establish guidelines, policies, and compliance are handled in a different manner as well.

Depending on the organization, what type of security is established or being created will depend on how they implement it. Hardware and software lifecycles have a much broader implementation plan than new employee security awareness training. The National Institute of Standards and Technology (NIST) publication 800-18 on Guide for Developing Security Plans for Federal Information Systems discusses ongoing system security plan maintenance and implementation. This methodology can be applied to not only federal systems, but in the private sector as well. During the implementation phase, the NIST outlines items that should be noted while implemented such as change in information system owner, change in information security representative, change in system architecture, change in system status, additions/deletions of system interconnections, change in system scope, change in authorizing official, and change in certification and accreditation status (Swanson, Hash, &

Bownen, 2006). Following guidelines of an implementation plan can ensure a smooth process that the plan will be a success.

Maintenance Plans

Maintenance plans would include policies, procedures, standards, guidelines, change management, and hardware/software lifecycles. All organization with any type of data of any classification, using any type of hardware or software will require some type of security maintenance plan. Whether or not a plan is enforced, written, or the organization lives by their plan is entirely up to them. Best practices show that a plan in effect can reduce costs, reduce security threats while increasing security overall, and provide a better working environment. Maintenance plans are established because they provide procedures, standards, and guidelines. Normally, without them, an organization might work in chaos mode or make hasty decisions on the spot that could compromise data, systems, and the organization. Security is vital to any organization. However, how that security is applied and implemented is just as important. It is one thing to think about a security plan for the organization, and it is another thing to develop, implement, and maintain security for the organization.

Conclusion

Any organization that engages in the usage, storage, and communication of data should understand the overall need for security management. Risk management is part of overall broad subject of security management. Understanding “risk” can guide the organization, through education, awareness, policies, procedures, and standards, to a better understanding how their organization views risk, what they do with risk, assessing risk, and managing it effectively. When undertaking risk management, a fully designed plan should evolve that will revolve around the organization and their operations. A smaller company might consider risk management as a low priority, while a large corporation would place an extremely high emphasis on risk management that is only a part of an overall security management program in place.

Risk management involves many categories of security for information technology. Risk assessment is the beginning of the management, which includes counting your assets and knowing what you have. Intellectual property is also just as important. An organization that does not know what they have cannot properly respond to incidents if something were to occur. Developing a business continuity plan is a large part of risk management. Having polices in place for change control, disaster recovery, and physical security can not only save the company money, but also save them legally. As with most public organizations, they might fall under some governing regulation which brings into risk management legal and ethical considerations. A hospital falling under HIPAA regulations is required by law to implement safeguards of data, and not doing such can jeopardize the organization. However,

all organizations, public or private, establish standards and ethics. Without standards and ethics, the risk level can increase, and compromised risks can be attacked. Lastly, and with any categories in risk management, a maintenance plan needs to be established. The maintenance plan will encompass policies, procedures, standards, and awareness. It is the summary of a risk management, that once in place; the organization has a full blueprint of the entire risk management plan.

References

ISO/IEC 17799:2005 Information technology. (n.d.). Retrieved May 30, 2008, from International Organization for Standardization: http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

Change Management (ITSM). (2008, October 22). Retrieved December 05, 2008, from Wikipedia: http://en.wikipedia.org/wiki/Change_Management_(ITSM)

Computer Life Cycle Management and Migration. (2008). Retrieved December 05, 2008, from OnTrack Data Recovery: http://www.ontrackdatarecovery.com/managing-computer-migration/

Confidential Data Handling Blueprint. (2008, October 14). Retrieved November 13, 2008, from Internet2.org: https://wiki.internet2.edu/confluence/display/secguide/Confidential+Data+Handling+Blueprint

Contingency Planning Guide for Information Technology Systems. (2002, June). Retrieved May 20, 2008, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

Defintion - Countermeasure. (2006, June 12). Retrieved November 14, 2008, from SearchSfotwareQuality.com: http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci1193329,00.html

Five ethical dilemmas IT leaders must confront. (2008). Retrieved November 29, 2008, from TechRepublic: http://video.techrepublic.com.com/2422-14074_11-216895.html

Harris, S. (2008). *CISSP Exam Guide* (4th ed.). New York, NY: McGraw Hill.

How to Develop a Risk Management Plan. (2008, October 14). Retrieved November 14, 2008, from Wikihow.com: http://www.wikihow.com/Develop-a-Risk-Management-Plan

How to terminate network administrator's employment? (2007, October 13). Retrieved October 18, 2008, from Firewall.cx: http://www.firewall.cx/ftopic-4913-0-days0-orderasc-.html

Incident Management Guidelines. (n.d.). Retrieved September 10, 2008, from Department for Business Enterprise and Regultory Reform: http://www.berr.gov.uk/sectors/infosec/infosecadvice/incidentmanagement/guidelines/page33389.html

Introduction to Risk Analysis. (2003). Retrieved October 31, 2008, from Security Risk Analysis

Direcory: http://www.security-risk-analysis.com/introduction.htm

Marking Classified National Security Information. (2007, October). Retrieved November 13, 2008, from National Archives: http://www.archives.gov/isoo/training/marking-booklet.pdf

NCSA Security Policies and Procedures. (2005, September 30). Retrieved December 05, 2008, from National Center for Supercomputing Applications: http://www.ncsa.uiuc.edu/UserInfo/Security/policy/NCSA_SPP.html

Risk Assessment Methodology Overview . (2008). Retrieved December 9, 2008, from University of California Office of the President: http://www.ucop.edu/irc/itsec/riskmethodology.html

Spafford, G. (2003, July 18). *The Importance of System Change Controls*. Retrieved November 14, 2008, from Datamation: http://itmanagement.earthweb.com/service/article.php/2237201

Swanson, M., Hash, J., & Bownen, P. (2006, February). *Guide for Developing Security Plans for Federal Information Systems.* Retrieved December 06, 2008, from NIST: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

Wikiepedia - Trade Secret. (2008, October 29). Retrieved October 30, 2008, from Wikiepdia: http://en.wikipedia.org/wiki/Trade_secret

Table of Figures