

Network and Security Analysis  
ABC Company

Justin Falk

# TABLE OF CONTENTS

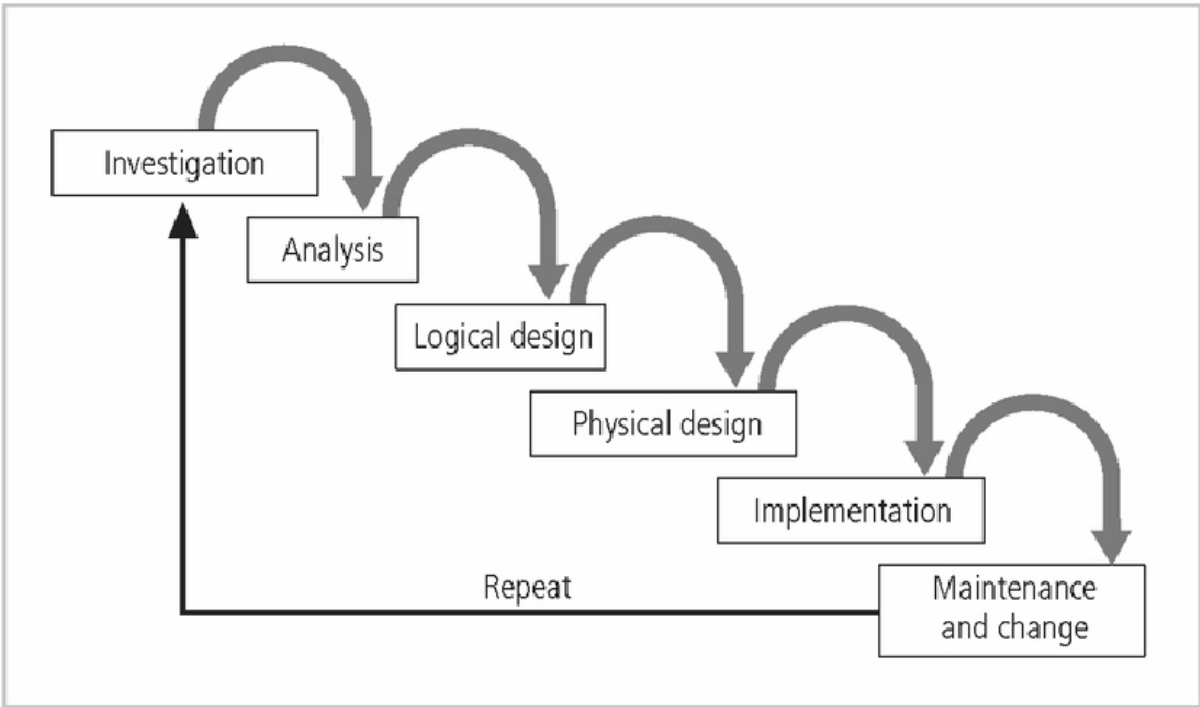
ABSTRACT: .....	3
INTRODUCTION .....	4
PROJECT TIMELINE .....	5
INVESTIGATION .....	5
PROBLEM STATEMENT AND BACKGROUND INFORMATION .....	6
SECURITY ANALYSIS .....	8
SECURITY DESIGN .....	12
Risk Solution Short Explanations .....	15
Design Proposals: .....	17
Active Directory Proposal .....	17
ISA Facts & Analysis .....	19
Desktop Protection Choices and Recommendation .....	21
Design Policies and Procedures: .....	23
Internet Usage .....	23
Company Phone Usage .....	25
Employee Termination and Guidelines .....	26
Employment Termination Checklist .....	26
Notification .....	27
Permissions Termination .....	27
Return of Property .....	27
Exit Interview .....	27
Computer Maintenance .....	29
Server Maintenance .....	31
Information Backup .....	32
Backup ISP Proposal .....	33
Identity Security Card Proposal .....	34
Video Surveillance Proposal .....	35
IMPLEMENTATION AND TESTING .....	36
CONCLUSION .....	36
Appendix A .....	36
REFERENCES .....	40

## **ABSTRACT:**

ABC Company has requested assistance for possible enhancements on their current network and security. This paper will discuss the needs of the company through information gathering, various analysis, and company feedback on past experiences. We will be performing the steps of the security development life cycle, focusing on full security analysis and design. The full project will consist of a request of information services that will discuss the client's expectations and areas of improvement followed by the network and security analysis, product research, policies, and proposals.

# INTRODUCTION

A small to medium sized company, ABC Company, is requesting help with their overall security and network design. This has initiated the security systems development lifecycle. Many experts consider the Security System Development Lifecycle (SecSDLC) to be “the best approach for implementing any information security system in an organization with little or no formal security” (Whitman, 2003.) Typically the development lifecycle is started from either an event-driven or plan-driven initiative. For this particular company a small series of event-driven incidents has caused the company to consider a plan-driven implementation of the lifecycle. Below is a chart of the typical stages in the lifecycle. This was used as a skeleton for entire project.



We began performing the steps of the security development life cycle, focusing on full security analysis and design with a specific focus in the client’s network. Before beginning the first phase a plan was set to regulate time stipulations to try to help gauge the scope.



# PROBLEM STATEMENT AND BACKGROUND INFORMATION



**Apollo Travel Management**

Phone: 312-236-3939  
 Fax: 312-236-3939

## REQUEST FOR INFORMATION SYSTEM SERVICES

DATE OF REQUEST	SERVICE REQUESTED FOR DEPARTMENT(S)
05/14/2007	Department of Information Technology

SUBMITTED BY (key user contact)	EXECUTIVE SPONSOR (funding authority)
<b>Name</b> Justin Falk, Anner Aquino <b>Title</b> Students <b>Office</b> Graduate Dept of Robert Morris <b>Phone</b> 219-614-4265, 773-882-6357	<b>Name</b> Housam Hajyousif <b>Title</b> IT Director <b>Office</b> Information Technology <b>Phone</b> 708-XXX-XXX

**TYPE OF SERVICE REQUESTED:**

- |   |   |
|---|---|
| <input type="checkbox"/> Information Strategy Planning  | <input type="checkbox"/> Existing Application Enhancement               |
| <input type="checkbox"/> Business Process Analysis and Redesign                                   | <input type="checkbox"/> Existing Application Maintenance (problem fix) |
| <input type="checkbox"/> New Application Development  | <input type="checkbox"/> Not Sure                                       |
| <input checked="" type="checkbox"/> Other (please specify: <u>Network and Security Analysis</u> ) |   |

**BRIEF STATEMENT OF PROBLEM, OPPORTUNITY, OR DIRECTIVE** (attach additional documentation as necessary)

There are many problems, opportunities and directives for Apollo Travel Agency. One of the biggest complaints of IT is the time spent in reconfiguring trouble equipment. This equipment is troubled due to numerous security problems including, malware intrusion, technology obsolescence, and other security threats. Currently in our conversations with Housam we have identified all backups are done manually. A previous experience caused the email server to be down for 3 days causing massive loss of reservations from other vendors and customers. The client currently uses peer-to-peer networking due to fear of changing to a domain. The client has numerous mobile users connecting remotely without a VPN technology. The client is dissatisfied with the functionality of the current firewall hardware. The client is currently using a proprietary substandard software program, called Zone Alarm to patch desktop computers only when they experience problems with malware. Client also uses Symantec for virus protection which also conflicts with Zone Alarm. Client has no existing DMZ for a multitude of servers located in the datacenter/server room. Client has no current documented security policies for employees regarding use of computers. All problems are dealt with by emails when experiencing a problem. Streaming of material such as multimedia streaming sometimes causes lack of bandwidth resulting in frustration and warnings from the IT department. There are no existing documents such as policies that we were able to obtain from the client. The client's server room does not have a UPS or proper Halotron fire extinguishers. There are no cameras monitoring the facilities which are also wide open to physical breaches of security. No keycards or locks are placed on the doors to the network or server room. We observed both doors left wide open. Client desktops often need reformatted from frequent build up of malware and viruses. Recently the CEO's computer was replaced with a new computer from a virus infection. Also due to the limited amount of time IT has because it is frequently tied up reformatting and configuring machines it has been giving employees and agents access to many security functions, especially if the employee has some computer savvy-ness. Before a line conditioner was implemented, a new IBM raid server was destroyed due to a power surge. One month's worth of data was lost and the system left rendered completely unusable. Client frequently battles technology obsolescence and replaces hard drives and machines randomly as they fail. Client doesn't really know what will fail next. No preventive maintenance is performed. Client also has no way of monitoring or discovering intrusions. Client requests some sort of intrusion detection system or software. Client has also lost many contracts or information from employees that are either terminated or leave the company. No existing policy outlines information stealing or right to non-compete agreements. Client has experienced a wide variety of worms, viruses, and even denial of service attacks. Client does have a Microsoft partnership allowing them to implement Microsoft software products for a very discounted rate.

**BRIEF STATEMENT OF EXPECTED SOLUTION**

Client would like analysis and recommendations for a firewall, gateway, or other intrusion detection system. A desktop recommendation is expected in regards to frequent problems with employee computers to battle viruses, malware, etc. If a VPN is possible using the clients CISCO 2600 router it would be desired to research how this is possible. Physical security suggestions such as cameras, keycards, and fire extinguishers will be outlined and recommended. Lastly, policies and documents will help tighten up overall security.

**ACTION (ISS Office Use Only)**

Feasibility assessment approved

Assigned to Justin Falk, Anner Aquino

Feasibility assessment waived

Approved Budget \$ Student Time

Start Date May 14, 2007 Deadline June 25, 2007

Request delayed

Backlogged until date: \_\_\_\_\_

Request rejected

Reason: \_\_\_\_\_

Authorized Signatures:

\_\_\_\_\_

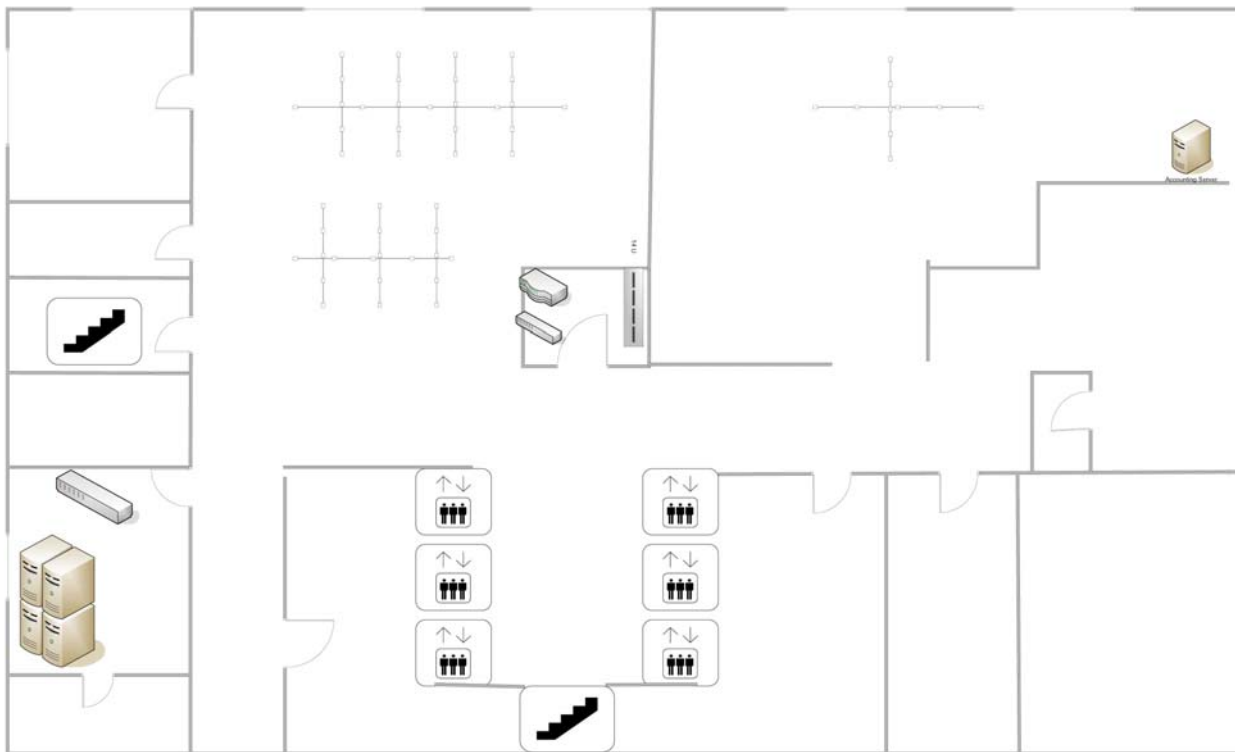
Housam\_ Hajyousif

**Project Executive Sponsor**

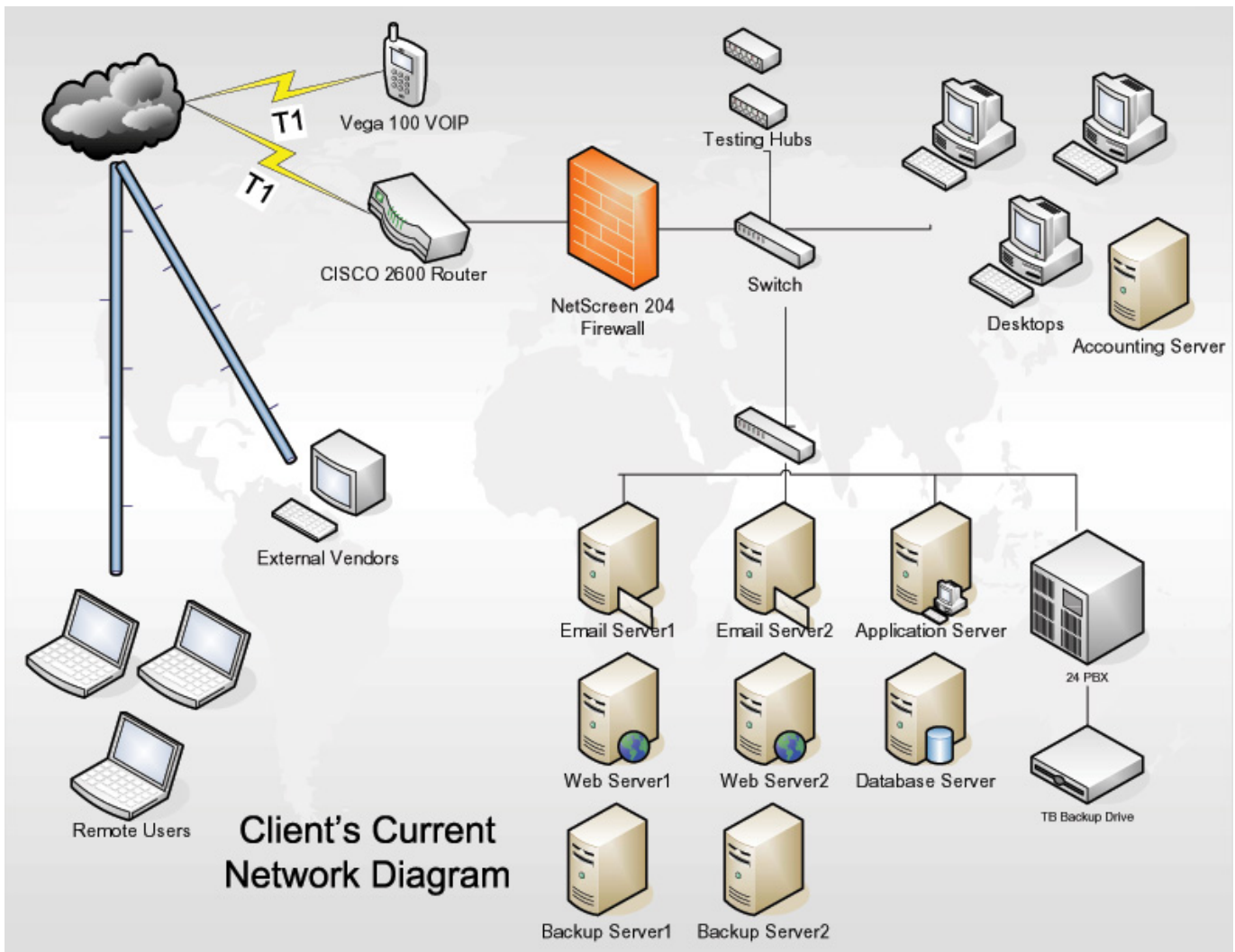
# SECURITY ANALYSIS

The analysis phase of the SecSDLC studies your information assets and likely threats to them. An asset is an “organizational resource” that has value, while a threat includes “an object, person, or other entity that represents a constant danger to an asset. The analysis primarily consists of assessments of the organization, the status of current systems, and the capability to support the proposed systems.” (Whitman, 2003) Here is the step to determining what the new security and network plan should be expected to do, and how it will interact with the current security setup and network. Current security policies, if any existed, were documented. Any legal matters or issues that could impact a future design were discussed. There were not any relevant issues that were found to affect the project. Asset identification and risk assessment were evaluated.

## Client Floorplan



Shown above is the client’s current floor plan created by our team, a necessary document in analyzing the physical security of any organization.



Shown above is the client's current network diagram in order to aid in the network and security analysis.

Asset Identification						
Legend	1 - Low	3 - Moderate	5 - High			
	40%	10%	25%	25%	100%	
Asset	Productivity Costs -	Replacement Cost	Protection Costs	Liabilities	Overall	weight
Netscreen 204	4	5	2	4	3.6	7.11%
Cisco 2600	5	2	1	3	3.2	6.32%
T1 lines	5	3	1	4	3.55	7.02%
Mail Servers	4	4	3	4	3.75	7.41%
Web Servers	4	4	3	4	3.75	7.41%
Backup Servers	1	4	3	4	2.55	5.04%
Application Server	4	4	3	4	3.75	7.41%
Database Server	4	4	3	4	3.75	7.41%
Desktops/Laptops	3	3	4	2	3	5.93%
PBX System	5	4	1	5	3.9	7.71%
Backup Drive	1	2	1	2	1.35	2.67%
Switches and Hubs	3	2	1	2	2.15	4.25%
Peripherals	2	1	2	1	1.65	3.26%
Proprietary Information	5	5	3	5	4.5	8.89%
Procedures and Policies	3	1	2	4	2.8	5.53%
People	3	4	3	4	3.35	6.62%

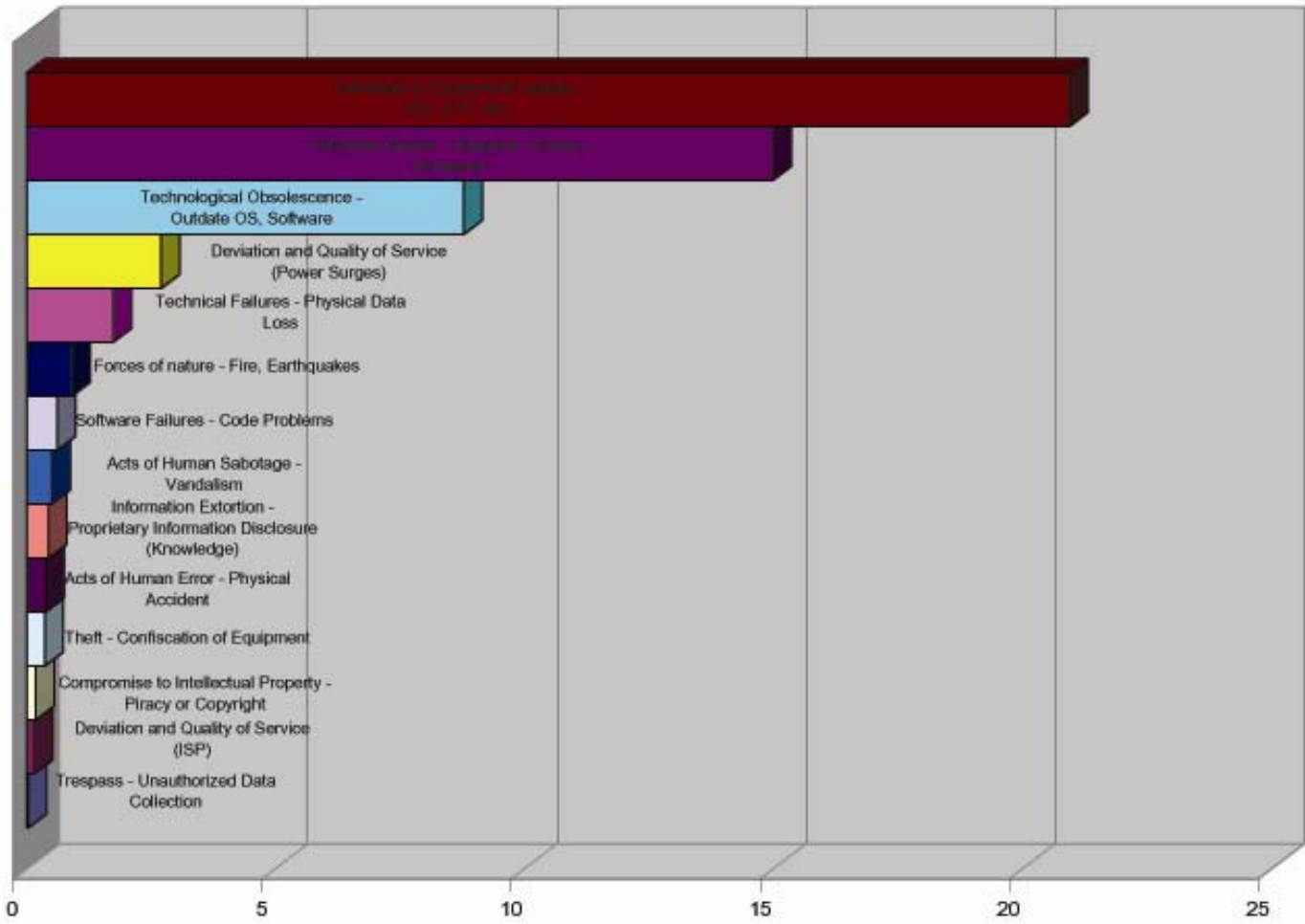
Asset identification was performed above in order to rank identified assets by importance to the organization. These assets were ranked on a scale of 1 to 5, 5 being of highest importance. Weight was given to the assets based on a variety of factors including productivity cost, replacement cost, protection cost, and liability.

RISK ASSESSMENT					
Severity	1 - Low	3 - Moderate	5 - High		
Risk Frequency	1 - Minimal	3 - Expected	5 - All of the time		
	50%	50%			
Risk Name	Severity of Risk	Risk Frequency	Overall	Risk Choice	Preferred Solution
Software Attacks - Malware, Viruses, Intrusions	3	5	4	Avoidance	Network Protection
Hardware or Equipment Failures - HD, CPU	3.5	3	3.25	Mitigation	Maintenance Policy
Information Extortion - Proprietary Information Disclosure	4	2	3	Mitigation	Policy
Forces of nature - Fire, Earthquakes	5	1	3	Mitigation/Acceptance	ND Equipment
Deviation and Quality of Service (Power Surges)	4	2	3	Avoidance	UPS
Technical Failures - Data Loss	4	2	3	Avoidance	Backup Policy
Deviation and Quality of Service (ISP)	4.5	1	2.75	Mitigation	Backup ISP
Acts of Human Error - Physical Accident	1	4	2.5	Avoidance	Locking Areas
Trespass - Unauthorized Data Collection	4	1	2.5	Avoidance	Security Cards/Cameras
Acts of Human Sabotage - Vandalism	4	1	2.5	Avoidance	Security Cards/Cameras
Theft - Confiscation of Equipment	4	1	2.5	Avoidance	Security Cards/Cameras
Technological Obsolescence - Outdate OS, Software	3	2	2.5	Acceptance	Patch Maintenance
Compromise to Intellectual Property - Piracy or Copyright	3	1	2	Acceptance	Policy/Encryption
Software Failures - Code Problems	3	1	2	Acceptance	Patch Maintenance

A preliminary risk assessment was performed based on risk severity and frequency. This was drafted based off current observations of the client's previous experiences and how they impacted the organization. However, this led to some minor bias in the imperativeness of the risk in regards to the IT department as compared to the overall organization.

<b>Risk Assessment</b>					
Risk Name	Risk Frequency	Assets affected	Impact	Percent Controlled	Risk
Software Attacks - Malware, Viruses, Intrusions	90%	Servers, Desktops	41.60%	60%	14.976
Hardware or Equipment Failures - HD, CPU	40%	Servers, Desktops, Netscreen, Cisco, Switches, Peripherals	61.56%	15%	20.9304
Information Extortion - Proprietary Information Disclosure (Knowledge)	15%	Proprietary Information, Procedures and Policies	14.43%	80%	0.4329
Forces of nature - Fire, Earthquakes	1%	All	100%	10%	0.9
Deviation and Quality of Service (Power Surges)	5%	Electrical Assets	71.94%	25%	2.69775
Technical Failures - Physical Data Loss	10%	Servers, Desktops, Backup Drive	43.28%	60%	1.7312
Risk Name	Risk Frequency	Assets affected	Impact	Percent Controlled	Risk
Acts of Human Error - Physical Accident	2%	Desktops, Peripherals, Proprietary Info., Procedures and Policies	23.62%	20%	0.37792
Trespass - Unauthorized Data Collection	2%	Proprietary Information, Procedures and Policies	14.43%	90%	0.02886
Acts of Human Sabotage - Vandalism	5%	All Assets	100.00%	90%	0.5
Theft - Confiscation of Equipment	5%	All Equipment	71.94%	90%	0.3597
Technological Obsolescence - Outdate OS, Software	20%	Servers, Desktops, Peripherals	43.87%	0%	8.774
Compromise to Intellectual Property - Piracy or Copyright	4%	Proprietary Information, Procedure and Policies	8.89%	50%	0.1778
Software Failures - Code Problems	3%	Servers, Desktops, Peripherals	40.61%	50%	0.60915

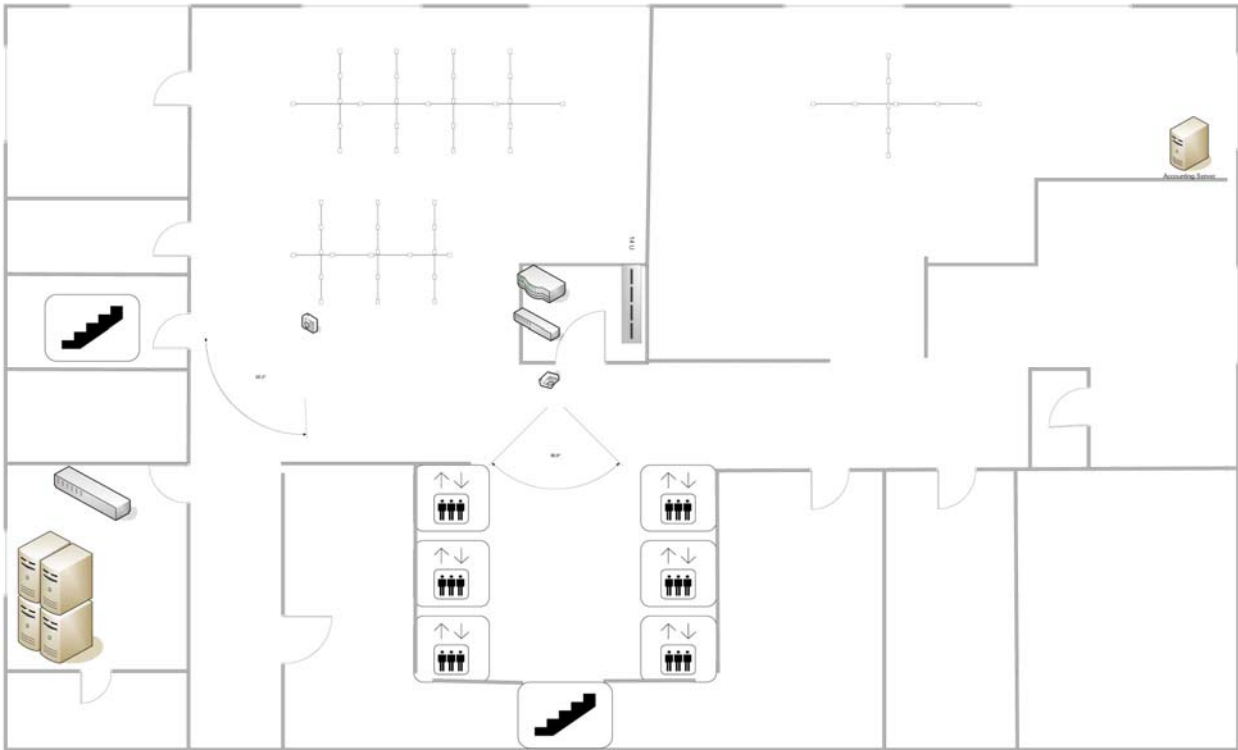
Due to the simple assessment causing some concerns a more careful analysis was designed to link to the assets to the risks for overall impact to the entire organization. Risk frequency was determined along with a formulated impact regarding which particular assets would be effected if the risk were to occur and how important those assets were to the organization as a whole. The formulated risk was calculated by multiplying the risk frequency by the asset impact by the percent uncontrolled (1 minus the percent controlled) for a total value of the risk. The risks are listed below in a graph format to display the criticality and aide in determination of our logical design for the project.

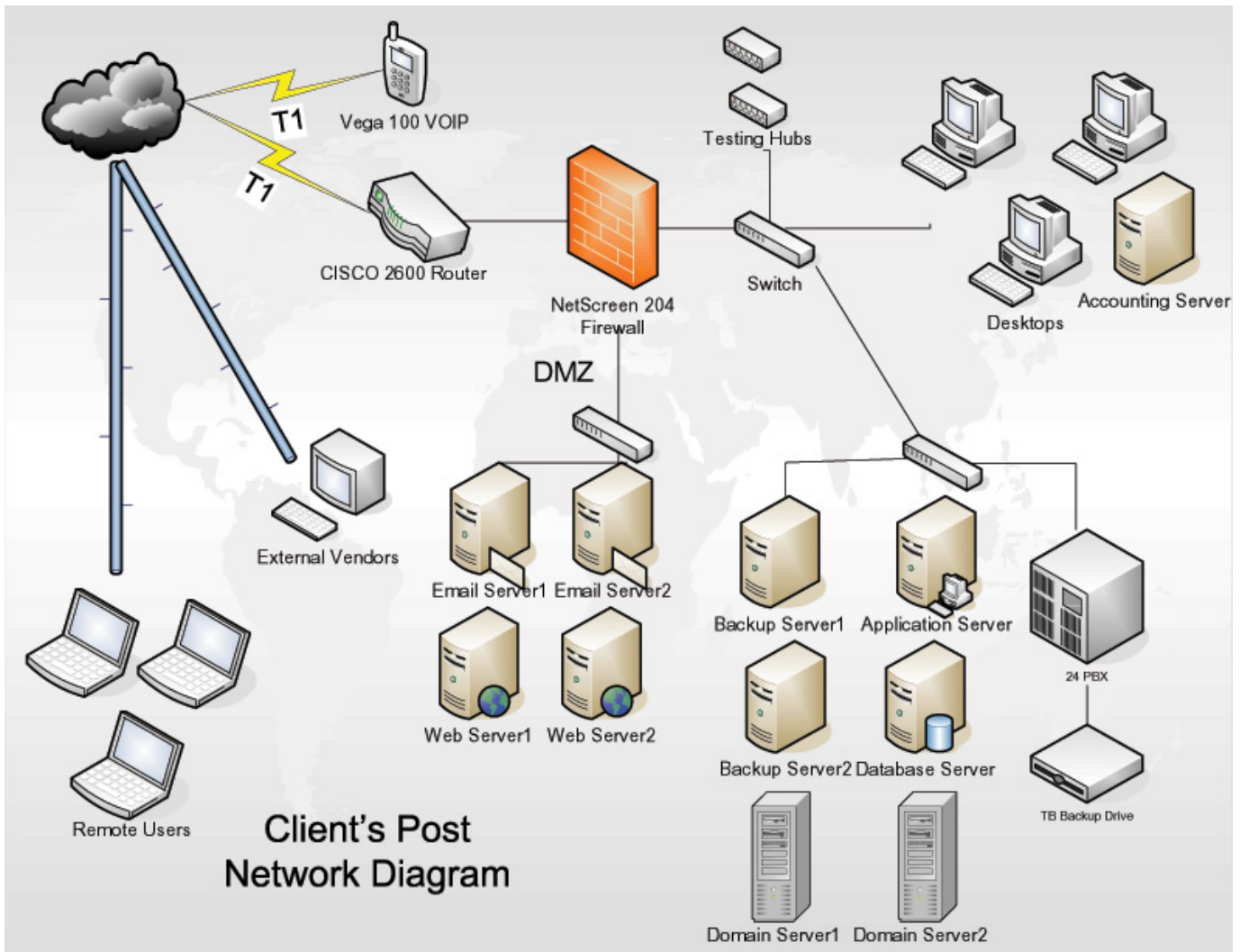


## SECURITY DESIGN

The primary goal of the logical design phase of the SecSDLC is “to “design an information security program. The creation of an information security program begins with an information security blueprint.” (Whitman, 2003) The following proposed floor plan and network diagram serve as an information blueprint to facilitate the physical design of the network and security plan. Typically, critical planning and feasibility analyses session should take place in order to determine whether or not the project should continue. In this case continuous meetings with faculty assisted in our analyses to continue with the project. The security technology was examined and design was placed in order of precedence in alignment with the client’s risks. Decisions were made in regards to develop a designed solution to either prevent, mitigate, transfer, or accept the current risks.

# Client Floorplan Video Surveillance





**Client's Post  
Network Diagram**

ABC Company  
Information Technology Division

**Risk Solution Short Explanations**

Software Attacks - Malware, Viruses, Intrusions	Avoidance	Network Protection
Hardware or Equipment Failures - HD, CPU	Mitigation	Maintenance Policy
Information Extortion - Proprietary Information Disclosure	Mitigation	Policy
Forces of nature – Fire, Earthquakes	Mitigation/Acceptance	ND Equipment
Deviation and Quality of Service (Power Surges)	Avoidance	UPS
Technical Failures - Data Loss	Avoidance	Backup Policy
Deviation and Quality of Service (ISP)	Mitigation	Backup ISP
Acts of Human Error - Physical Accident	Avoidance	Locking Areas
Trespass - Unauthorized Data Collection	Avoidance	Security Cards/Cameras
Acts of Human Sabotage – Vandalism	Avoidance	Security Cards/Cameras
Theft - Confiscation of Equipment	Avoidance	Security Cards/Cameras
Technological Obsolescence - Outdate OS, Software	Acceptance	Patch Maintenance
Compromise to Intellectual Property - Piracy or Copyright	Acceptance	Policy /Encryption
Software Failures - Code Problems	Acceptance	Patch Maintenance

**Software Attacks – Malware, Viruses, Intrusions**

To prevent these types of events desktop protection software, Deep Freeze by Faronics, is recommended. Deep Freeze Server Edition can also be used with client’s servers. Deep Freeze allows for a quick and instant fix of software problems by simply rebooting the computer. The computer will boot with a previously saved image despite any recent changed files from reconfigurations, viruses, etc. The software can be deployed and controlled remotely and has flexibility to save specific files or changes users may need to perform in their job activities. Virus software should be updated with most current definition updates. Also, a close examination of the clients hardware firewall should be performed to ensure it is being used to its full ability to restrict intrusions. A domain server(s) should be setup to implement active directory and better control the desktops. This would allow for quick and easy permission settings, restrictions, etc with current users. This would also allow for configuration of an application gateway such as Microsoft ISA for enhanced network security as well as an intrusion detection system.

**Hardware of Equipment Failures – HD, CPU**

To prevent these types of events a strict policy or equipment chart should be followed. Care should be taken in logging purchases of equipment and a routine periodic review should be performed to check for aged equipment. If possible purchases should be done in tandem with the same equipment to make maintenance simpler. If equipment fails a backup should be ready for quick redundancy while original equipment is restored or replaced.

**Information Extortion - Proprietary Information Disclosure**

To better help losing close relations with business partners or possible dissemination of confidential information an employee termination policy and checklist should be implemented. By following this procedure client may be less likely to be exposed to this type of situation from former employees.

**Forces of nature - Fire, Earthquakes**

Client should have at least some minimal type of natural disaster equipment such as proper fire extinguishers. Also data should be backed up off site or remotely.

**Deviation and Quality of Service (Power Surges)**

Power surges happen occasionally and must be controlled. Client already has some surge protection equipment in the form of a line conditioner. More equipment may need to be purchased to suppress spikes for most important assets or all assets. An uninterruptible power supply should highly be considered for purchase for temporary loss of power.

**Technical Failures - Data Loss**

A simple backup policy should be implemented to prevent data loss or time involved in restoring backups. Backups should be performed frequently and automatically if possible.

**Deviation and Quality of Service (ISP)**

In the event that the Internet Service Provider is not able to provide service the client would desperately need to a contingency plan. Purchasing a backup ISDN line is recommended due to its “pay as you use cost” and bandwidth sufficient for temporary use.

**Acts of Human Error - Physical Accident**

Certain areas of client worksite should be restricted. By requiring some form of authorization or simply using current locks and doors would prevent many human related accidents in these areas.

**Trespass - Unauthorized Data Collection**

Acts of Human Sabotage – Vandalism

Theft - Confiscation of Equipment

All of these risks can hopefully be avoided with use of security cards, locks, and cameras within the premises.

**Technological Obsolescence - Outdate OS, Software**

In regards to software obsolescence not too much can be done that is worth the time and effort of the IT staff. Replacement of software with known problems or issues should be done immediately to prevent future complications. Also patch maintenance or automatic updates should be performed with software and operating systems.

**Compromise to Intellectual Property - Piracy or Copyright**

Not much can be done to help battle this risk that is worthwhile. Informing employees of sensitivity of information or not allowing people to know all pieces of information may help prevent a compromise to intellectual property. Encryption should be used for any network functions with sensitive data.

**Software Failures - Code Problems**

All software is subject to bugs or code problems. If certain issues are discovered there may be updated versions of software available. Patch maintenance may also help with software problems. Also known software vendors support numbers and information should be kept in a centralized document.

# Design Proposals:

ABC Company  
Information Technology Division  
**Active Directory Proposal**

## *Objective:*

The objective of this proposal is to establish active directory for the client's network.

## *Problem Statement:*

ABC Company has to constantly reconfigure machines due to configuration changes, intrusions, viruses, malware, and hardware failures.

## *Overview:*

Active Directory is the integrated, distributed directory service that is included with Microsoft Windows Server 2003 and Microsoft Windows 2000 Server.

AD would provide a more secure and manageable environment to make the lives of the IT staff at ABC much easier. With Active Directory, ABC organization can add a user to Active Directory and through that single entry enable remote access to the network, enable the same user account for Exchange messaging, that same user for database access for accounting, client relationship management, or other applications.

## *Benefits:*

### **Authentication Access**

Once a user logs in to Windows at ABC their Active Directory credentials will automatically unlock all of the applications or services that they have been enabled for, including 3<sup>rd</sup> party applications that utilize Windows integrated authentication.

### **Group Policy**

- Allows the administrator at ABC to centrally configure and administer system, user, and application settings.
- Push out a software update or utility to all desktops and laptops remotely. (Laptops may often not be accessible from field employees for weeks at ABC)
- Set user settings such as home directories, default settings, or configuration settings.
- Lock down and even hide functions that users do not need to access.
- Patched and updated systems prevent users from getting viruses or worms that can have dramatic impact on user productivity and potentially the loss of critical information from a workstation or network drive.

Instead of having IT staff at ABC spend an entire week walking from computer to computer to install an update or make system configuration changes this can be done from one central location.

### **Remote Assistance**

Allows a user to request assistance from an administrator or support resource to help with technical issues they are encountering. The support resource can be granted the ability to remotely control the desktop and take control of the system to perform troubleshooting and administrative tasks, without having to be physically at the user's keyboard. This is especially useful when supporting remote users of ABC who might be at their home office, or in the field, other countries, etc.

### **Future VPN protection**

Network Access Quarantine Control, available in the Windows Server 2003 Resource Kit, can be used to delay remote access (VPN connection) to an organization's network until the remote system has been

examined and validated for proper patches, updates, and anti-virus signature files. A script is then run on the computer and if it verifies the computer is running an approved configuration then the quarantine mode is removed and the computer is granted normal access to the network resources.

By testing and validating systems for the most recent updates and anti-virus definitions, ABC can be spared problems from users who remotely connect to the network and inadvertently spread viruses and worms through their remote VPN connection.

### **IPSec**

IPSec is a mechanism for establishing end-to-end encryption of all data packets sent between computers. IPSec is built-in to Windows Server 2003 and allows all communications out of the network adapter to be sent in a 168-bit encrypted format.

With a matched client and server encryption connection, users can be assured that the conversations and data transmitted between the IPSec server and the ABC client laptops are as private and secure as possible.

### **Password Policies**

ABC can create policy to enforce password history (how many passwords are remembered), maximum password age in days, minimum password length in characters, and whether passwords must meet specific complexity requirements.

By creating and enforcing password policies for ABC, the administrators of the network can ensure an appropriate policy has been set for the organization to meet the standards and requirements expected of the organization and further enhance its security and protection of its assets.

### **Software Restriction Policies**

ABC can create a policy that restricts access and/or execution of application software.

For example, ABC can restrict users from email viruses if they are worried about potential users receiving viruses through e-mail.

A policy setting can be applied that does not allow certain file types to be executed on a system. This way if there is a known virus on the network, the software restriction policy settings can be used to stop computers from opening the file that contains the virus. The ability to allow and deny user access to certain applications will help ABC in its desktop protection problem.

### **Advanced Server Recovery**

ASR facilitates the restoration of a failed server, and reduces the amount of time an administrator needs to spend building and reconfiguring a new server.

It is a recovery utility that allows a server administrator to rebuild a failed server without having to reinstall and reconfigure the operating system.

In the event of a server failure for ABC, assuming the replacement server has the exact hardware configuration, which is true for many servers in ABC; ASR can be used to rebuild the system as it was before the failure.

### **Encrypted File System**

EFS would be especially useful for securing sensitive data on portable computers for ABC. For example if a laptop is stolen and the thief removed the hard drive and attempted to read the encrypted files on another computer, they would not be accessible.

### **ISA 2003**

With AD implemented ABC would be able to install ISA 2003, a comprehensive firewall and intrusion detection system package to compliment its hardware NetScreen 204 firewall.

## ISA Facts & Analysis

In contrast to a packet filter hardware device, you need *real* firewall protection. Simple packet filtering is inadequate when it comes to protecting resources within the network. Not only must you be able to insure that all incoming connections are subjected to deep application layer inspection, you must also control what leaves the asset networks using strong user/group based access control.

In contrast to a typical hardware packet filtering firewall that lets everything out, the firewalls at the network edge must be able to control outbound connections based on user/group based membership. Reasons for this include:

- You must be able to log the user name of all outbound connections so that you can make users accountable for their Internet activity
- You must be able to log the application the user used to access Internet content; this allows you to determine if applications not allowed by network use policy are being used and enables you to take effective countermeasures
- Your organization may be held responsible for material leaving your network; therefore you must be able to block inappropriate material from leaving your network
- Sensitive corporate information may be transferred outside the network from Asset Network locations. You must be able to block this and record user names and applications the users are using to transfer proprietary information to a location outside your network

The ISA Server 2004 firewall is the ideal firewall for the network edge because it meets all of these requirements. When systems are properly configured as Firewall and Web Proxy clients, you are able to:

- Record the user name for all TCP and UDP connections made to the Internet (or any other network that the user might connect to by going through the ISA Server 2004 firewall)
- Record the application the user uses to make these TCP and UDP connections through the ISA Server 2004 firewall
- Block connections to any domain name or IP address based on user name or group membership
- Block access to any content outside their network based on user name or group membership
- Block transfer of information from the Asset Network to any other network based on user name or group membership

All this deep application layer stateful inspection and access control requires processing power. That's why you should size your servers appropriately to meet the requirements of powerful stateful application layer processing. Fortunately, even with complex rule sets, the ISA Server 2004 firewall is able to handle well over 1.5 gigabits/second per server, and even higher traffic volumes with the appropriate hardware configuration.

## Why ISA Belongs in Front of Critical Assets

- ISA Server 2004 firewalls run on computer hardware, which keeps costs in check while allowing you the luxury of upgrading the hardware with commodity components when you wish to "scale up" the computer platform that ISA Server 2004 firewall runs on
- Being a "software" firewall, the firewall configuration can be quickly upgraded with application aware enhancing software from Microsoft and from third-party vendors
- Being a "software" firewall, you can quickly replace broken components without returning the entire firewall to the vendor.
- The ISA Server 2004 firewall provides sophisticated and comprehensive application layer filtering, in addition to stateful packet filtering. The stateful application layer and stateful packet filtering protect against common network layer attacks and modern application layer attacks
- The ISA Server 2004 firewall should be placed behind high-speed packet filtering firewalls if you have a very high speed connection to the Internet. This is especially important on networks with multi-gigabit connections. The packet filtering firewalls reduce the total amount of traffic each back end ISA Server 2004 firewall needs to process. This reduces the total amount of processing overhead required on the ISA Server 2004 firewalls and allows the ISA Server 2004 firewalls to provide the true, deep application layer stateful inspection required to protect your network assets
- While the ISA Server 2004 firewall can't match the pure packet passing capabilities of traditional hardware ASIC based firewalls, the ISA Server 2004 firewall provides a much higher level of firewall functionality via its stateful packet filtering and stateful application layer inspection features
- The ISA Server 2004 firewall is able to authenticate all communications moving through the firewall. This provides for strong user/group based authentication to and from the vital asset networks.

## Desktop Protection Choices and Recommendation

- **Centurion Guard**

*Vendor:* Centurion Technologies

*Website URL:* <http://www.centuriontech.com/centurionguard.htm>

*Description:*

The Centurion Guard. Hard Drive Protection Device protects your system by write protecting the hard drive at the physical level, similar to the way you write protect your floppy disks by setting the write protect tab. When an application needs to write to the hard drive, the Centurion Guard automatically redirects file writes to a separate non-write protected area on your hard drive. When the system is rebooted, any changes that were made to DOS or Windows are forgotten, and the system is put back to its default configuration.

*Cost:* 1-24, \$84; 25-99, \$79; 100-299, \$74; 300-499, \$69; 500-999, \$64, 1000+, Call

- **DriveShield**

*Vendor:* Centurion Technologies

*Website URL:* <http://www.centuriontech.com/driveshield.htm>

*Description:*

DriveShield is the new software based laptop/PC hard drive protection from Centurion Technologies, Inc. It allows anyone to reset a system back to its original configuration with a simple reboot. DriveShield write protects the hard drive at the physical sector level, similar to the way you write protect your floppy disk by setting the write protect tab. When an application needs to write to the hard drive, DriveShield automatically redirects file writes to a separate non-write protected area on your hard drive. When the system is rebooted, any changes that were made to Windows are forgotten and the system is restored to its default configuration.

*Cost:* 1-24, \$39.95; 25-99, \$37.95; 100-299, \$35.95; 300-499, \$33.95; 500-999, \$31.95, 1000+, Call.

- **Deep Freeze**

*Vendor:* Faronics Inc.

*Website URL:* <http://www.faronics.com/html/deepfreeze.asp>

*Description:*

Deep Freeze "freezes" your software configuration. Whatever hackers, mischief makers and innocent clickers attempt, their "work" will instantly disappear when the computer is restarted. All settings, files and programs are 100% restored to their original configuration every time. Deep Freeze requires NO setup or configuration. Just install, restart and its working. Save files to a floppy, network, or into a specified Deep Freeze "thawed" space. It's easy to make permanent changes; just turn Deep Freeze off and install or remove your programs or make configuration changes.

*Cost:* Educational Pricing (K-12): Single Workstation license, \$ 39.95; 15 workstation per building license, \$ 268.00; 100 workstation per building license, \$475.00; Unlimited use per building license, \$ 575.00

## **Recommendation**

We chose to recommend Deep Freeze because of how simple it was to setup, its high amount of features, expanded flexibility, and cost efficiency with the number of licenses the client would need.

If you can setup Group Policies in a Windows 2000/XP environment and use Deep Freeze along with it, this not only saves considerable money, but also provides a large amount of security and reliability. The Group Policies lock down your machines and Deep Freeze adds another layer of security so a restart fixes any problem a user might have gotten into. Another plus is that Deep Freeze is simple. Since IT staff is limited only a quick restart is required if a PC is in trouble. During a restart, Deep Freeze clears all passwords and other sensitive information off the computer, thereby allowing users to use on-line banking, etc., without having to worry having discovering of their passwords. If you purchase the Enterprise version of Deep Freeze, you can turn on the computers, shut them down, freeze or thaw them, all from one PC. You can also easily update machine configurations without having to "touch" each one. This prevents a person having to go to each machine to apply updates, new virus definitions, etc. And the latest version of Enterprise allows you to setup and point machines to a Software Update Server (SUS), a free product from Microsoft that pushes out updates to machines at a specified time. This saves tons of time and protects the network from new vulnerabilities found in Windows and other Microsoft products.

As described above in the short explanations, policies and proposals were created as part of the design efforts of enhancing the network and security practices of the client. Listed below is our individual policies which could easily be adopted by the client.

## Design Policies and Procedures:

ABC Company  
**Internet Usage**  
 Policy and Procedure

<b>Policy Title:</b>	Internet Usage		
<b>Policy Number:</b>	1.0	<b>Effective Date:</b>	July 01, 2007
<b>Purpose:</b>	The ABC Company maintains intranet and internet access for its employees for the purpose of improving productivity, professional development, and the level of service to the clients of the company.		
<b>Regulation Reference:</b>			
<b>Prepared by:</b>		<b>Approved by:</b>	

### 1.0 Policy

The ABC network (which includes company-owned or leased local and wide-area networks, the internet and the World Wide Web, and the computers connected to them, hereafter referred to as “the system”) is not a public access service, nor is it a public forum. The ABC Company has the right to place reasonable restrictions on the material you access or post through the system. You may not use the system for commercial purposes. This means you may not offer, provide, or purchase products or services through the ABC system, except for products or services directly related to your official duties.

### 2.0 Objective

This document outlines proper and improper use of the internet and computers provided to all employees of ABC Company.

### 3.0 Scope

This policy also applies to all company provided access to the internet or other computers and computer networks.

### 4.0 Procedure

#### **Unacceptable Uses**

The following uses of the ABC system are considered unacceptable:

- ☞ Inappropriate Access to Material - You will not use the ABC system to access material that is designated for “adults only” or is profane or obscene (pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (hate literature).

- ☞ Inappropriate Language Restrictions - No electronic communication messages should be created or sent that may constitute intimidating, hostile or offensive material on the basis of race, color, creed, religion, national origin, age, sex, marital status, lawful alien status, non job related physical or mental disability, veteran status, sexual orientation, or any other basis prohibited by law. ABC's policy against sexual or other harassment, including same sex harassment, applies fully to electronic communications.
- ☞ Improper Access or Hacking - You will not attempt to gain unauthorized access to the company system, or to any other computer system through the ABC company system, or go beyond your authorized access. This includes attempting to log in through another person's account or access another person's files. You will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. You will not use ABC system to engage in any other illegal act.
- ☞ System Security - You are responsible for your individual account and must take all reasonable precautions to prevent others from being able to use your account. Under no conditions should you provide your password to another person. You will immediately notify the system administrator if you have identified a possible security problem. (Do not go looking for security problems, because this may be construed as an illegal attempt to gain access.)
- ☞ Copyright - You will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner.
- ☞ Unsafe Material - All computers are vulnerable to viruses, therefore you should not download anything from any site you are not convinced is safe. Any attachment to an e-mail received from an unknown source should be scanned for virus prior to opening it.
- ☞ Other Illegal Activity - You will not take any other action by or through the system or any part of the system which is otherwise illegal, including, but not limited to gambling, trafficking in narcotics or the making of threats.
- ☞ Personal Use is not prohibited, in accordance with the other terms and conditions of this policy. Employee may use the computer for personal use after hours, however all the rules listed in policy apply.

**Privacy:**

The ABC Company reserves the right to monitor your use of the system and any communications. Routine maintenance and monitoring of ABC system may lead to discovery that you have violated this Policy, work rules, or the law. In the ordinary course of its business and for legitimate reasons of management or of security, the company may, at its sole discretion and without prior notice:

- a) peruse, read, copy, reproduce, print, use, communicate, keep, move, store or destroy, in whole or in part, the information, messages, files or data located in the Internet network access system, whether or not such information, messages, files or data have been created, received or kept by the user with the help of said system;
- b) monitor, in real or deferred time, using any technical means, access to the Internet network and the use thereof by the user, whether or not the user is aware of being monitored;

5.0 Revision History

ABC Company  
**Company Phone Usage**  
 Policy and Procedure

<b>Policy Title:</b>	Company Phone Usage		
<b>Policy Number:</b>	2.0	<b>Effective Date:</b>	July 01, 2007
<b>Purpose:</b>	To describe the employee termination policy and procedures of ABC Company. The following policies and procedures apply to all employees of ABC Company.		
<b>Regulation Reference:</b>			
<b>Prepared by:</b>		<b>Approved by:</b>	

1.0 Policy

The ABC Company provides telephone access to all employees. Abuse of the telephone use policy can result in disciplinary actions.

2.0 Objective

This document outlines proper and improper use of the telephone access provided to all employees of ABC Company.

3.0 Scope

This policy also applies to company provided cell phones including during non-business hours.

4.0 Procedure

Abuse includes, conducting personal business during work hours, receiving or making excessive personal phone calls, making phone calls to "adult lines" and disclosing confidential information over the phone. As a general rule, employees are discouraged from making or receiving personal telephone calls through the ABC telephone system. The ABC Company does recognize that under certain circumstances, an employee will need to make or receive a telephone call of a personal nature from a business phone. Those calls must be held to a minimum in both time and number.

5.0 Revision History

## Employee Termination and Guidelines

### Policy and Procedure

<b>Policy Title:</b>	Employee Termination and Guidelines		
<b>Policy Number:</b>	3.0	<b>Effective Date:</b>	July 01, 2007
<b>Purpose:</b>	To describe the employee termination policy and procedures of ABC Company. The following policies and procedures apply to all employees of ABC Company.		
<b>Regulation Reference:</b>			
<b>Prepared by:</b>		<b>Approved by:</b>	

#### 1.0 Policy

There are three broad principles to which adherence is required when and after terminating an employee.

- Prompt notification of termination.
- Information security should entail researching, documenting, and revoking an employee's access to the company's electronically stored proprietary information and its information systems.
- Prudent revocation of access.

In the case of an employee whose end of employment is only imminent, IT should consult with the employee's manager, HR, and other key decision-makers to determine the appropriate manner in which to stagger the revocation of access over the person's remaining days of employment.

#### 2.0 Objective

This document outlines the termination procedures. The revocation of access should be documented, especially for legal purposes. The goal, of course, should always be to revoke access in ways that make good business sense financially, technologically, and legally.

#### 3.0 Scope

This policy applies to all company employees and assets including those electronic.

#### 4.0 Procedure

### Employment Termination Checklist

Employee Name: \_\_\_\_\_

Date: \_\_\_\_\_

## Notification

\_\_\_\_\_ **Notify:** As soon as you are aware of and/or receive a letter from an employee that notifies you of the employee's intention to terminate employment, notify Information Technology office.

\_\_\_\_\_ **Official Notice:** If an employee tells you of their intention to leave your employment, ask them to write a letter that states their resignation and their termination date.

(We request a minimum of two weeks notice, when possible and desirable.)

\_\_\_\_\_ **Preservation:** Conserve certain technological resources, data, and logs in the event that the former employee or company itself decides to pursue litigation.

## Permissions Termination

\_\_\_\_\_ **Notify Your Network Administrator:** As soon as you know that an employee is leaving, notify your Network Administrator or other appropriate staff person of the date and time on which to terminate the employee's access to computer and telephone systems. Make arrangements for how these accounts will be routed to ascertain that your organization will not lose contact with clients and customers.

IT should immediately revoke all computer, network, and data access the former employee has. Remote access should also be removed, and the former employee should be dispossessed of all company-owned property, including technological resources like a notebook computer and intellectual property like corporate files containing customer, sales, and marketing information.

## Return of Property

\_\_\_\_\_ **Return of company property:** Exiting employees are required to turn in all company books and materials, keys, ID badges, computers, cell phones, USB memory devices, and any other company-owned items.

\_\_\_\_\_ **Passwords:** Employees should provide their supervisors with passwords and other information pertaining to accessing computer files and telephone messages. (You may want to keep email and phone accounts active for awhile to field customer contacts.)

## Exit Interview

\_\_\_\_\_ **Confidential exit interview:** Exiting employees are encouraged to participate in a confidential exit interview with the Human Resources department. (Exit interviews are an important process you can use to gather information regarding the working environment in your organization. When notified that an employee is terminating employment, your office will schedule an exit interview. All information gathered is confidential and is reported periodically in summary form.

\_\_\_\_\_ **Written permission for reference checking:** Exiting employees, who plan to seek employment, must sign a form giving the company permission to provide reference information when potential employers call.

5.0 Revision History

ABC Company  
**Computer Maintenance**  
 Policy and Procedure

<b>Policy Title:</b>	Computer Maintenance Policy		
<b>Policy Number:</b>	4.0	<b>Effective Date:</b>	
<b>Purpose:</b>	Define procedures for obtaining and providing maintenance, service, or technical support for desktop computers, laptops, peripherals, and network devices.		
<b>Regulation Reference:</b>			
<b>Prepared by:</b>		<b>Approved by:</b>	

### 1.0 Policy

ABC Company shall follow standard procedures when performing computer or hardware maintenance. This will implement preventative practices and minimize computer and hardware downtime and assures production will not be affected.

### 2.0 Objective

This document outlines a procedure to enable an assigned user to perform any necessary maintenance on computers or hardware devices.

### 3.0 Scope

Maintenance will be performed on the following:

- Company owned computers or laptops
- Company owned printers
- Company purchased software applications
- Hardware devices such as Printers, Switches, Hubs, etc.

### 4.0 Procedure

1. If a problem occurs with a desktop computer or laptop, the user must contact the IT Staff at (312) 555-5555 or e-mail@domain.com

2. IT Staff personnel will determine whether the nature of the problem is related to the network, software, or hardware and will take necessary actions to resolve the issues.

3. Hardware repairs may be performed by a third-party service provider. If a hardware problem exists, IT Staff will generate a trouble ticket that includes the following information:

1. Contact person (primary and secondary), phone number(s), and location
2. Account number (for billing purposes).
3. Equipment model/manufacturer and serial number(s).

4. Departments with desktop computer equipment may be able select the equipment's service options (annual maintenance, warranty) that best services or support their particular requirements. Departments can discuss with Administrators regarding service alternatives, but should be aware that third party repair contracts are limited in scope. Third party repair technicians must abide by company security policies.
5. IT staff will contact the third-party service providers. The service providers will then contact the user to arrange the date and time for the service appointment.
6. IT staff will communicate any necessary maintenance, such as patches, that will enable security via e-mail. E-mail will include the following:

What: Microsoft XP and Office 2003 security patches for ABC Company workstations

When: Starting Day, Month ##, 2007 6:00pm local time

How: Systems Management Server (SMS) is the tool used for patching and software upgrades. SMS automates downloading and installation on each workstation after IT has reviewed, tested, and approved the list of items to be applied. SMS works in the background, so you may never even see that it's updating your system. In some circumstances, you may see one or more pop ups related to the updates taking place (on the taskbar, lower right corner of your screen). These pop ups will be dependent on how up-to-date your system is and what patch is being installed at that time. You will probably receive a pop up balloon advising that a reboot is needed. Patches may require a reboot of systems. Although you have the option to reboot at any time, we do recommend that you do it as soon as possible. Please note: If you see any pop ups noting an action needed other than a reboot, please contact the IT staff to determine your next steps.

Why: Patching is necessary to keep our computers as safe as possible from a variety of security issues, and like virus protection, up-to-date patch levels are required for every system that connects to the Thomson network. This effort ensures the ongoing health and protection of our network. It is imperative we keep our systems and servers virus and spyware free.

If you have any further questions about this process, please contact the IT Service Desk.

Email: e-mail@domain.com

Phone: 312-555-5555

5.0 Revision History

ABC Company  
**Server Maintenance**  
Policy and Procedure

<b>Policy Title:</b>	Server Maintenance Policy		
<b>Policy Number:</b>	5.0	<b>Effective Date:</b>	July 01, 2007
<b>Purpose:</b>	Define procedures for server maintenance.		
<b>Regulation Reference:</b>			
<b>Prepared by:</b>		<b>Approved by:</b>	

#### 1.0 Policy

ABC Company shall follow standard procedures in order to assure servers are fully up to date.

#### 2.0 Objective

This document outlines a procedure to enable an assigned user to perform any necessary maintenance servers.

#### 3.0 Scope

Maintenance will include the following:

- Installation of latest security and vulnerability patches
- Monitor disk and memory usage
- Assure virus definitions are up to date
- Keep record of age of disk drives
- Records maintenance of servers

#### 4.0 Procedure

1. IT department is fully responsible for patching vulnerabilities of server security
2. IT department will update virus definitions and assure virus scan is working properly
3. Assure surge protectors are protecting servers.
4. Perform maintenance according to set schedule.
5. Maintenance will occur every Sunday at 00:00:00PM
6. IT department will make necessary communication before maintenance.
  - a. IT department will include a WHAT, WHEN, HOW, and WHY sections when sending communication e-mails.

#### 5.0 Revision History

ABC Company  
**Information Backup**  
Policy and Procedure

<b>Policy Title:</b>	Information Backup Policy		
<b>Policy Number:</b>	6.0	<b>Effective Date:</b>	July 01, 2007
<b>Purpose:</b>	To provide a step by step approach to perform data backups in compliance with established policies		
<b>Regulation Reference:</b>			
<b>Prepared by:</b>		<b>Approved by:</b>	

#### 1.0 Policy

It is the objective of ABC Company to adopt IT industry best practices. Therefore, it is a requirement of the Information Technology department to ensure all critical data is securely backed up on a set schedule.

#### 2.0 Objective

This document outlines a procedure to enable an assigned user to perform scheduled data backups.

#### 3.0 Scope

Backup will be performed on all data and application servers. Full data backup will automatically be performed according to set schedule.

#### 4.0 Procedure

Each server must be configured to automatically start a batch backup process. According to current procedures, data should be backed up to tape drive Sunday evenings unless otherwise requested by IT department. Backup tapes should contain a label with the date of backup. Tapes will be held for X amount of time.

##### User Data:

All data on server's shared directories will be backed up during the schedule backups.

#### 5.0 Revision History

ABC Company  
Information Technology Division  
**Backup ISP Proposal**

*Objective:*

The objective of this proposal is to establish a backup Internet Service Provider in the case of an unexpected dedicated-line outage.

*Problem Statement:*

A current backup Internet Service Provider does not exist. This can be crucial if employees are unable to connect to external applications or obtain external resources to conduct business.

*Background:*

ABC Company experienced an outage that caused downtime of over 3 days. During these days, much business was lost. The current ISP has an average uptime of 99.9%, however any downtime can have a negative effect on productivity.

*Benefits:*

Obtaining a backup ISP can assure projects get done when the dedicated-line fails. This can become a life saving option when critical projects or business is on the line.

*Method:*

Dial-up option: No one wants to go back to dial-up speed to download, upload, or search for information on the web, but when it is the only option available, this method becomes imperative.

*Typical Product Functions and Features:*

- Pay for usage only or get cheap monthly rate
- Pop e-mail accounts
- Works on various Operating Systems

*Sources:*

Dial-up services can be obtained but are not limited to the following sources:

[www.easycall.net](http://www.easycall.net)

[www.550access.com](http://www.550access.com)

[www.megapath.com](http://www.megapath.com)

*Price:*

\$9.99

*Schedule:*

ABC Company  
Information Technology Division  
**Identity Security Card Proposal**

*Objective:*

The objective of this proposal is to establish an identity security card system in the areas of main elevator lobby and server rooms. Regardless of the security that is currently available, we would like to suggest adding additional layers of protection.

*Problem Statement:*

ABC Company currently does not have the secure identity solution and contactless smart card technology for physical access control that they would like to have. Restrictions to premises or server rooms have not been implemented with technology. Typically, large scale companies have such systems embedded within their premises and have set a security model for smaller companies.

*Benefits:*

Being able to have proof of who entered the premises and when the occurrence happened can help investigate theft, vandalism, tampering, and other disasters of similar nature. The system can also help verify employee time of arrival.

*Method:*

Based on research of ten anonymous, large and small, companies, HID Corporation has been the security card company preferred. Companies surveyed were all based in Chicago and were randomly selected. HID Corporation would manage installation and configurations.

*Typical Product Functions and Features:*

**HID PROXIMITY**

Operating Frequency: 125 kHz

Format Size: Up to 84 bits

Read Range: Up to 24" (60cm) depending on local installation conditions and card reader selection.

*Design:*

Security readers will be placed on the elevator lobby area and server rooms. Readers will be placed at the point of entrance and in a visible position. See post floor diagram.

*Resources:*

<b>Provider</b>	<b>Contact</b>	<b>Website</b>	<b>Recommendation</b>
HID Corporation	800-872-5359	www.hidcorp.com	X
Bosch Security Systems	585-223-4060	www.boschsecurity.com	
International Electronics	781-821-5566	www.ieib.com	

ABC Company  
Information Technology Division  
**Video Surveillance Proposal**

*Objective:*

The objective of this proposal is to establish a video surveillance system that will provide additional security at ABC Company in order to reach the next level of protection.

*Problem Statement:*

The office is set up with a security guard at the front entrance. When entering the building, a visitor must sign in and show proof of identification to the guard. Visitors must sign out when leaving the premises. It is possible that during a visit, a person can look for alternative ways to enter the building during off hours.

*Benefits:*

A video surveillance system provides the information needed when company assets are at stake. This is beneficial and important when trying to identify or investigate trespassers and thieves. The cost of a video surveillance system are much less than the cost of theft or vandalism.

*Methods:*

1. ADT's ViewPro Video Surveillance solutions or
2. Brink's CCTV Surveillance services or
3. In-house surveillance.

*Typical Product Functions and Features:*

Solutions from companies such as ADT or Brinks help deter theft, detect fraudulent liability claims and documents events for the organization. Other solutions such as the "do it yourself" may be affordable, but having to maintain a server to record activity may add additional responsibilities to the network staff.

*Design:*

The video surveillance cameras should be placed by the entrances of the company premises. It is suggested to install 1 camera on the North and 1 on the South of the elevator area. Additional cameras may be required near windows of server room.

*Hardware:*

Cameras: Dome or Box - varies resolution  
Monitors: Color or flat panel monitors  
Power Supplies: AC Adapters  
Cables/Connectors: BNC Cables  
Distribution Amplifiers: Distribute video lines  
UPS: Used for CRT Monitors

*Resources:*

[www.ati247.com](http://www.ati247.com)  
[www.adt.com](http://www.adt.com)  
[www.brinks.com](http://www.brinks.com)

*Schedule:*

Typical implementation schedule

Week1	Week2	Week3	Week4	Week5
Research				
	Contact			
		Installation		
			Testing	
				Evaluation

## **IMPLEMENTATION AND TESTING**

The entire project should be presented to upper management and project stakeholders for review and implementation. In this instance the client was contacted for presentation and consideration of many of these design solutions. Care was taken by the team to test configuration and implementation designs such as the client desktop configuration protection software. Due to the nature of this project and limitations of access to the client site much of the implementation testing was performed on dummy machines and terminals. Testing was also performed during many parts of the design stage for feasibility tests including the ease of implementation and the ease of maintenance in regards to a limited IT staff. Having these stages of the lifecycle overlap was found to help with choosing solutions as well as recommendations for proposal to the client.

## **CONCLUSION**

The task of securing a network can be quite a difficult, costly, and time consuming. It is however a task that must be completed before the unexpected occurs. By utilizing the SecSDLC, ABC Company can implement solutions that have been researched through this project. After implementation, the company can rest feeling assured that many of the vulnerabilities have been resolved.

## **Appendix A**

Detail of Business Functions:

*Needs:*

*Applications (Types or Services):*

*Profit Revenue:*

Scope of Project (Expectations):

*Client view:*

*Group view:*

IT Composition (Staff) and Policies (Regulations):

*Documentation:*

\*Background checks

Network Infrastructure (Overview):

*Documentation:*

Assets:

*Human Resources:*

*Physical:*

*Logical (Data, Trademarks):*

Main Concerns:

Past Experiences:

*Costs:*

**TABLE 2-1** Threats to Information Security<sup>4</sup>

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Security Measures and Approach (Bottom Up/Top Down):

*Flexibility/Sensitivity:*

*Maintenance (Obsolescence):*

*Balance:*

Information Characteristics:

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

Providers:

**Additional Information:**

Clients/Servers:

Server Types:

Network Type:

Traffic Patterns:

Firewall Type:

Security Applications:

\*Include E-mail

VPN (Encryption):

DMZ (Groups or Servers):

Design Goals (General):

## REFERENCES

- 550Access, 550Access Regular Dial-up, <http://www.550access.com>, Accessed: June 10, 2007
- ADT, Video Surveillance, <http://www.adt.com>, Accessed: June 5, 2007
- Aventura Technologies, Products and Equipment, <http://www.ati247.com>, Accessed: June 5, 2007
- Bosch, Bosch Security Systems Worldwide, <http://www.boschsecurity.com>, Accessed: June 1, 2007
- Brinks, Brink's Business Security, <http://www.brinks.com>, Accessed: June 5, 2007
- Centurion Technologies, Driveshield, <http://www.centuriontech.com/products/driveshield/>, Accessed: June 07, 2007
- Centurion Technologies, Centurion Guard, <http://www.centuriontech.com/centurionguard.htm>, Accessed: June 07, 2007
- EasyCall Communications, Dial-up Internet, <http://www.easycall.net>, Accessed: June 10, 2007
- Faronics, DeepFreeze, <http://www.faronics.com/html/deepfreeze.asp>, Accessed: June 11, 2007
- HID Corporation, HID Proximity, <http://www.hidcorp.com>, Accessed: June 1, 2007
- International Electronics, Inc., Access Control, <http://www.ieib.com>, Accessed: June 1, 2007
- ISA Server Org, ISA Firewall Fairy Tales, <http://www.isaserver.org/articles/2004tales.html>, Accessed: June 12, 2007
- Megapath, Megapath Duet, <http://www.megapath.com>, Accessed: June 10, 2007
- Microsoft Corporation, Active Directory Benefits for Smaller Enterprises, Whitepaper, Published September 2004
- Ortmeier, P.J, Security Management: An Introduction (2nd Edition), 2006
- US Data Trust, Backup Servers, <http://www.usdatatrust.com>, Accessed: June 10, 2007
- Whitten, J. L, Bentley, L., Systems Analysis and Design Methods (Seventh Edition), 2005.
- Whitman, M. Mattord, H. (2003). Principles of Information Security. Boston, MA: Thomson Learning, Inc.