Global Information Assurance Certification Paper

GIAC Enterprises GDS

GIAC Program Practical
Information Security Officer Training
GISO – Basic Practical Assignment
Version 1.2 (February 2002)
Submitted by Kurtis E. Kroeckel

Abstract/Summary:

This practical deals with the Global Distribution Service (GDS) industry. This industry handles reservations. The network is described for how tour operators, travel agencies, and travel web sites retrieve their needed information. Remote users are part of the network and described on how they connect. The suppliers that update the reservations have their network connections described. A little is touched on the mainframe security. The author's policy is examined. The new policy is very specific on distributed server security.

Table of Contents

Assignment 1 – Describe GIAC Enterprises

Description of GIAC Enterprises

At GIAC Enterprises it is our business to provide the travel industry with the most reliable and accurate access to inventory and pricing information.

GIAC Enterprises have the expertise that airlines, car rental companies, cruise lines, hotel properties, rail lines, tour operators and travel agencies around the world depend on because of the years we have in the industry. This is why we are one of the world's fastest growing providers of electronic global distribution services. We are connecting approximately 10,000 travel agency locations to 250 airlines, 10 car rental companies, 25,000 hotel properties, 120 tour operators and all major cruise lines throughout the world.

Our strong staff of approximately 1500 professionals takes a truly unique approach in supporting our business. Our employees understand that technology is what makes us who we are, and unfailingly make customer service the highest priority. Customer satisfaction must and is our ultimate goal.[1]

GIAC Enterprises is a Global Distribution Service (GDS) organization. Reservations are our commodity and the core of our business. A reservation represents a seat on a passenger airline, a seat on a train, a bed on a cruise liner, an automobile, or a bed in a hotel. These items are supplied to us through our suppliers. A supplier will be the entity that has the physical space or item available. The supplier is the Airline Company, hotel property, car rental agency, cruise line, or passenger Rail Company.

GIAC Enterprises brings a reservation together for the travel Business Company and their customer. A travel business company is the tour operator, travel agency, or travel web site. The travel Business Company has customers that need the reservation that the supplier has. GIAC Enterprises is the medium used to create the connection between the supplier's reservation and the travel Business Company's customer request. The transaction of reserving the time slot for the particular available seat, car, or bed for the travel Business Company's customer is the reservation.

This is how GIAC Enterprises receives revenue. Revenue is dependent on the amount of reservations sold. When a travel business company creates or changes a reservation for their customer within our system, revenue is generated for each transaction. GIAC Enterprises enjoys revenue for each transaction.

IT Infrastructure

Products Overview

The security for the OS/390 operating system mainframe is handled by the CA-ACF2 security product release 6.3. CA-ACF2 security controls VM user access to the VM system. CA-ACF2 security controls access to the VM minidisks and CMS files. CA-ACF2 security will control access to the terminals, CP commands and diagnose instructions, and other types of user-defined resources. This includes applications and OS/390 data sets. The CA-ACF2 security adds Standard Security Facility (CAISSF) technology to the CA-CIS Integration Services, allowing centralized security administration and auditing through a single security facility. Having one security facility helps maintain control over this environment.[2]

Security for the DB2 version 2.3 database is handled by CA-ACF2 for DB2 version 1 release 1. CA-ACF2 for DB2 has a single-point for centralized security strategy. This simplifies the complex process of managing access to any critical DB2 resources, privileges and utilities. In providing the consistent security and logging, all auditing and reporting is made easier. These advantages are brought into the DB2 environment."[3]

Throughout the Intranet, the majority of the routers used are Cisco 7206s. The IOS for the Cisco 7206 is NPE 225. The Cisco 7206 is a multi protocol (ip, ipx, decnet, etc.) capable router. GIAC Enterprises is using the ip protocol only but we do have the flexibility for a supplier or other outside source that would need to connect to the Intranet using a different protocol. The Cisco 7206 has six slots and it will support multiple protocols. It can route multimedia and bridging over a wide variety of Local Area Networks and Wide Area Network interface types. These functions bring the versatility that is needed within our network environment.[4]

All LAN interfaces (ports) require unique hardware addresses that are known by the MAC-layer addresses. Typically, the MAC address of an interface is stored in a memory component. This component usually is directly on the interface circuitry. The Cisco router OIR feature allows the port or service adapter to be removed and replace the port or service adapter with an identically configured one. The system recognizes that this is the same port or service adapter and will configure it and bring it online immediately. The reason this can be done is that Cisco stores the unique MAC address in an EEPROM on the router midplane. There is no confusion for the Cisco router because the MAC addresses are reserved for a specific port and slot in the router. The MAC addresses are assigned in sequence. This feature allows for the network to be stable. Another feature of this is that the port adapter or service adapter can be taken out and put into another router without confusing the network about the MAC address. The port adapter or service adapter will take on the new MAC address for that slot that is stored in the EEPROM of the router it is installed in.[5] This capability of replacing the port adapter with the same MAC address is important. The network will not suffer as long of an outage with this technology and every minute the network is down potentially thousands of dollars are loss.

And if needed, a lightly used router can have a port adapter or service adapter taken out and put into the failed router for a temporary fix.

There are two ATM switch routers used for the core of the Intranet. The switch routers used are the Cisco Catalyst 8540 MSR. The IOS for the Cisco Catalyst 8540 MSR is IOS release 12.1 (11b) E. The ATM switch router has a 13-slot modular chassis. The ATM switch router has dual power supplies. They are fault-tolerant and load sharing in either AC or DC power supplies. The dual router processors occupy the 4th and 8th slots. The processors are field-replaceable. They perform central processing functions and also provide the redundancy needed for the highly available network needed within the environment. The ATM switch router provides switched ATM connections to individual workstations, servers, LAN segments, or other ATM switches and routers using fiber-optic, unshielded twisted-pair (UTP), and coaxial cable. This is the type of flexibility needed within this complex environment.[6]

There are two types of firewalls in use within the Intranet. The first type is the Secure Computing Sidewinder firewall. GIAC Enterprises is using Dell hardware and purchased the software only. We have a preferred vendor solution in place with Dell. The hardware for the Secure Computing Sidewinder firewall is the Dell PowerEdge 6650 installed with the required hardware from Secure Computing.[7] The Secure Computing Sidewinder firewall SecureOS version 5.1.0.01 provides a number of options. One option is the tunable filtering that provides Application Level Proxies for the highest level of traffic control. Another option can be the circuit proxies for moderate levels of control. The Sidewinder also will do stateful packet filtering to maximize throughput for the network. The Sidewinder firewall uses Type Enforcement technology. This is a patented protective feature built into Sidewinder's SecureOS. It provides a layered internal defense that makes it impossible for an attacker to penetrate and subvert a Sidewinder.[8]

The second type of firewall is from CheckPoint. It is the FireWall-1 product. The hardware will be the appliance version. The management console is installed on a Dell PowerEdge 6650 running Microsoft Windows 2000 Server. The FireWall-1 product enables enterprises to define and enforce a single security policy that is comprehensive and protects all the network resources. The architecture delivers a highly scalable solution and will integrate into all aspects of network security. Cisco has patented a Stateful Inspection technology within this product.[9]

The EMAIL server for GIAC Enterprises is the product Microsoft Exchange 2000 Server. The server hardware is the Dell PowerEdge 6650 running Microsoft Windows 2000 Server. This will help improve the communication with suppliers, travel agencies, and tour operators and travel web site owners. The communication technology in Exchange allows us to communicate effectively within our organization with real-time access to information. This increases the

opportunity to better serve the suppliers, travel agencies, and tour operators and travel web site owners.[10] The Exchange Email Server is located within the core.

GIAC Enterprises has chosen the Microsoft VPN solution that includes the Point-to-Point Tunneling Protocol (PPTP). The users who will be connecting through the VPN are using Microsoft Windows 2000 Professional. This protocol is built into the Microsoft products that our remote users use. Our remote users establish an Internet connection. They use their built-in Microsoft products Point-to-Point Tunneling Protocol. PPTP enables the secure transfer of data from a remote computer to a private server by creating a VPN across the Internet. PPTP supports on-demand, multi-protocol, and virtual private networking over the Internet. With this protocol, our VPN data is secure as if we were part of the local network.[11]

Microsoft Internet Security and Acceleration Server (ISA) 2000 is used to set up and secure a virtual private network (VPN). It is the Microsoft product that has support for the VPN secure gateway. The VPN extends the private network of GIAC Enterprises so we have the access from the Internet. The VPN enables data to be sent between two computers across the Internet in a manner that emulates the properties of a point-to-point private link. The ISA Server is configured as a VPN server to support secure client-to-gateway remote access communication over the Internet.[12] This is how the VPN server within the DMZ at GIAC Enterprises is configured. The hardware is the Dell PowerEdge 6650 running Microsoft Windows 2000 Server.

IT Flow

GIAC Enterprises has a number of different entry points into the internal network. There are entry points through the Internet for tour operators, travel agencies, travel web sites, and employees. There are entry points directly into the internal network for tour operators, travel agencies, and suppliers. Certain safeguards are taken at strategic entry/exit points.

The mainframe contains the DB2 reservation database. The hardware, operating system and versions were discussed earlier. The reservations are manipulated through transactions from all outside sources. The outside sources are the suppliers, the travel agencies, tour operators, and travel web sites that are our customers. The IBM AIX RISC 6000 system hardware is the pSeries 690 with AIX version 5. This high-end hardware is needed for the amount of transaction processing that comes through this connection. The TCP/IP to ESCON IBM AIX RISC 6000 systems translate the TCP/IP packet that contains the transaction or data heading to the mainframe into an ESCON packet. The ESCON packet takes the encapsulated transaction or data and delivers the packet to the mainframe for some type of processing like data query, update, etc.

Reservation inventory within the DB2 database is kept up to date with direct connections from the suppliers to our Intranet. The suppliers' traverse a Cisco 7206 router. This segment has a Sidewinder firewall connected. This Intranet segment is secured with a Sidewinder firewall to allow only certain systems, TCP/IP address ranges, and ports from the supplier to connect to specific systems within the Intranet. After the TCP/IP packet is allowed through the Sidewinder firewall, the TCP/IP packet enters the Cisco 8540 Catalyst Switch. The TCP/IP packet leaves the Catalyst Switch and will arrive at the AIX TCP/IP to ESCON encapsulating server. Remember that the TCP/IP must be converted into ESCON before the DB2 database can be manipulated which resides on the mainframe.

Travel agencies and tour operators access the DB2 mainframe reservation system a couple of ways. The first way to connect to our Intranet is through a direct connection. This method is used for the larger travel agencies. The TCP/IP packet traverses through a Cisco 7206 router and passes through a Sidewinder firewall before ending up at the Cisco 8540 Catalyst Switch. From here, the TCP/IP packet leaves the Catalyst Switch and arrives at the AIX TCP/IP to ESCON encapsulating server. The mainframe DB2 database can be manipulated once the information gets into the mainframe realm.

The second way a travel agency or tour operator accesses the reservation mainframe is through the Internet. The Web Server is located within the Web Demilitarized Zone (DMZ). The hardware is the Sun Fire 6800 running Solaris 2.8. The Web application is the Sun One Web Server version 6. This is used because this product "provides the foundation and security necessary to build, manage, and maintain mission-critical Web sites and enable Sun[tm] ONE customers to provide a consistently high quality of service (uptime) to their end users."[13]

The travel agency or tour operator goes through an ISP that routes the TCP/IP traffic to us. The TCP/IP traffic enters our Web Demilitarized Zone (DMZ) through a Cisco 7206 that has a Sidewinder Firewall located on the segment. The decision to proxy the network information was that security is more important than network throughput. This very difficult decision was made along with the applications must be tuned for network optimization.

Our e-business allows travel web sites to book reservations connecting to our Sun One Web Server version 6. The Sidewinder firewall proxy the web server address to the Internet. This Sidewinder answers up on behalf of the web server sitting in the web server demilitarized zone. There is a CheckPoint firewall between the web server demilitarized zone and the internal network. This allows for only certain TCP/IP addresses and ports to enter into the application zone for processing. The network design of a web zone, application zone, and database zone further protect the core network through a layered defense.

The corporate demilitarized zone is used for the Simple Mail Transfer Protocol (SMTP) version 8.11, VPN, and external DNS systems. The SMTP is located on a Sun Fire 3800 with Solaris 2.8. The SMTP server forwards email outbound to the Internet. The incoming email arrives here and is filtered before going to the Microsoft Exchange Server 2000. The Symantec product Norton AnitVirus for Gateways 2.5 is used.[14] This product does SMTP filtering in the DMZ before the mail is allowed through. The VPN solution is done using the Microsoft ISA product. This was discussed in the Product Overview section. The Domain Name Service (DNS) is run on a Dell PowerEdge 6650 running Microsoft Windows 2000 Server using the DNS service. There is a Sidewinder firewall that will proxy for each system. The Sidewinder interfaces have aliases set up on both the Intranet and Internet. The Sidewinder proxy function translates the internal and external addresses and only allows for certain ports to traverse. There is a CheckPoint firewall between the corporate demilitarized zone and the internal network. This allows for only certain TCP/IP addresses and ports to traverse between the application zone, web zone and core network.

There is a section of network that sits between the demilitarized zones and the internal network. This is where the database and application servers sit. The Travel Agencies database server is on an IBM pSeries 660 model 6M1 running AIX version 5.1. The database is DB2 Universal Database version 8.1. The Financial database server is on an IBM pSeries 660 model 6M1 running AIX version 5.1 with the DB2 Universal Database version 8.1. The Development database server has two instances on it to reflect the Financial and Travel Agencies databases. It also is on an IBM pSeries 660 model 6M1 running AIX version 5.1 with the DB2 Universal Database version 8.1. There is a CheckPoint firewall between this network and the demilitarized zones and also between the core network. This segregates and allows tighter controls for these server functions from the demilitarized zone areas and internal network. The Travel Agencies database contains which travel agencies and tour operators are our customers. It contains addresses, discounts and other relevant facts about each one. The Financial database contains transaction information on what type of discounts are allowed with the different suppliers for the different travel agencies, tour operators, and travel web sites.

There is a section of network that sits between the demilitarized zones and the internal network. This section is different than the database section. It is the application section. This is where the Home Grown, Financial and Development Application servers sit. The Home Grown Application Server is on an IBM pSeries 660 model 6M1 running AIX version 5.1. It has the VisualAge C++ that runs on AIX. This is what is used for the Home Grown applications. The Financial Application Server is on an IBM pSeries 660 model 6M1 running AIX version 5.1. It has the WebSphere Application Server software that can handle e-business transactions quickly and smoothly, with the ability to access enterprise systems and create dynamic Web content.[15] This enables our business to create transactions quickly which is how we improve the bottom line.

The Development Application server is on an IBM pSeries 660 model 6M1 running AIX version 5.1 with both the WebSphere Application Server software and the VisualAge C++. The Financial Application server will take the reservation and pull the financial discounts for the valid travel agencies and tour operators and access the needed information from the databases. The Home Grown Application server will run queries against the DB2 mainframe to get information and tie it to the Financial Database. This is done a lot for the Travel Web sites since they did not fit into the original business model.

The corporate network where the internal DNS server and the employees have their computers sits within the core network. The internal DNS server is on a Dell PowerEdge 6650 running Microsoft Windows 2000 Server. The mainframes and the systems that support connectivity to them are part of this network section. Development and production processes are contained here also.

Employee remote access is through the VPN. The remote user logs on to the ISP. The remote user makes the connection to the ISA server and authenticates. The secure connection is made and the remote user now can do what is needed because of the secure connection. The remote user now is like being local on the LAN.

Business Operations

The bottom line to GIAC Enterprises success is to bring together a customer who needs to make travel arrangements with the reservation that is available from our suppliers. Our suppliers are the airlines, car rental agencies, hotels, cruise lines, and rail. Our customers are the travel agencies, tour operators, and individual travelers. Our product that we sell is the reservation. Our key to being successful is to never have reservations not available do to our mistake. That is any system that supports access too, or connectivity too the DB2 reservation mainframe will never go down. This means there has to be redundancy in every critical system including multiple network paths. The network must be available all the time.

The DB2 reservation system is critical to our business and is housed on the mainframe. Direct access to the reservation system must be given to our suppliers so they can keep their reservation records synchronized with their records within our reservation system. The supplier connections must have redundant network paths into the mainframe reservation system so the synchronization can happen. Another critical system is the TCP/IP to ESCON. This system is what allows the TCP/IP traffic to be encapsulated and enter the mainframe. Remember that this all happens in real time.

The Sun One Web Server is critical to our operation because this allows Internet access to the DB2 mainframe reservation system. Travel web sites, tour

operators, and travel agencies alike will connect to the Web Server to purchase or change travel arrangements. It must be an easy and enjoyable experience; otherwise, these customers will find alternate means to book their reservations for their customers which will result in revenue loss for us. The critical path for the web server is to and from the Internet. The network path to and from the application zone is critical also. Dealing with the Intranet is the DNS server. This is critical for any Intranet connectivity to our site. It must be available all the time.

The tour operators and travel agencies that have direct access to our Intranet are critical. This critical path is from the direct connection to the application zone. This is where the direct path and web path joins. The application zone area contains the Home Grown Application server and the Financial Application server. These servers take the requests from the tour operators and travel agencies that either come in directly to the network or the web requests that are from the travel agencies, tour operators, and travel web sites. The application servers talk to the database zone and then send the transaction on to the mainframe. All these server zones within the network must be up and available since these zones all deal with the transaction. The transaction is the reservation. Any point that is down be it a server or network will hurt the financial bottom line.

Assignment 2 - Identify Risks

Areas of Risk
Risk 1 – unauthorized access to private data

Personal Identifiable Information (PII) is transferred between the travel agency, tour operator, travel web site, supplier and our site continually. This information may contain credit card numbers and dates and times of reservations for individuals. This information is confidential and is at risk when it traverses the network. Another type of information that is at risk is user ID and password combination traversing the network insecurely. The threat of these types of information (PII, user ID/password) being examined by an unauthorized program sniffing the network needs to be mitigated.

The data within the private network is not secure. A developer could log on to one of the application servers or database servers. Even easier would be to log on to the development servers since these do not have as tight of control on them as the production. A sniffer program like tcpdump that is standard on AIX or snoop on Solaris can be used to look at the network traffic. This information can be redirected to a file and analyzed. This would not take a lot of effort. The developer could sift through the file looking for user name and password combinations of authoritative users like root, database administrator, or the application owner. With this information, the developer could do whatever because the authority would now be in the developer's grip. He/she could log on to the server that the user id is for and be that powerful user. More information

could be gathered easily to find PII information by putting in rouge code capturing credit card information. To hack into the site and get on one of the database servers or application servers would not be as easy but there is some risk.

Business sensitive data is stored within the databases. Travel agencies, tour operators, and travel web sites pay different rates for different packages. Our competitors do the same thing. If a competitor could get a hold of the different rates, they could adjust theirs accordingly. This would cause us to lose travel agencies, tour operators, and travel web sites because they will go to the competition because of pricing discounts.

Another area that is very crucial is the router configuration. The developer or hacker could see a router password. This person could log on to the router or switch and disable it by changing configurations or shutting it down. This would affect the network segment and all the systems on that segment. If one of the switches is compromised, that affects the majority of the network.

Along these lines but not as sinister is the developer wanting to put in some code that he/she feels is necessary. With the powerful userid and password combination, he/she could install the code. This code has not been approved and could cause problems for the system and possible the network. Again, the network must be responsive and available.

The final risk in this area for PII is the reservation itself. Again, if a person can sniff the network and find a reservation for a Very Important Person (VIP) or dignitary, a terrorist could use this small but important piece to plan a sinister attack. VIPs could be Federal, State, or Local Senators or Congressmen or elected officials. VIPs can be foreign nationals within a foreign country. Reservations are for airlines, hotels, rental cars etc. If all or one piece of the itinerary can be found, how easy is it to plan an attack around this piece of PII information. The sinister person has a date, time and location at his/her disposal.

Programs that are standard within an operating system that can sniff the network must have their permissions changed so only a super or authoritative user can have access to the program. Another option is to remove the program. I would lean to the permission change because this type of program is used to help solve network problems.

Secure Shell for SSH would go a long ways in securing the user id and password combination situation. All the Cisco routers and switches at the current IOS do support SSH. The PII data with the reservation and any credit card numbers need to be encrypted. HTTPS will work in the web environment. The developers will have to modify the home grown applications to access the databases and TCP/IP to ESCON servers using the Secure Shell for SSH port and tunneling the application through it. Unfortunately, there is not a way to encrypt the ESCON traffic at this point.

Risk 2 – applications not at vendor-supported levels

Another area of risk is applications and operating systems not at vendor supported levels. Vendor supported level code be it operating system or application is code that the vendor will support. If a problem or bug is found from some user, the vendor will correct by patching or incorporating into a new release. Non-supported Vendor code is code that will no longer be corrected by patching or allowing support calls for. This does not mean that the latest software version for the application or operating system is loaded. If an application or operating system is not compliant with a supported vendor level, the threat of a new virus, denial of service or other malicious code could leave the application or operating system without a vendor supported fix. Vendors do not correct problems for code that is not supported because it would be too costly. Along this line of thinking is that applications and operating systems need to be at the latest security releases for the software version that the vendor has released to limit the threat of malicious code.

Hackers gain a lot of access into networks because the proper patching of the operating system or application has not been done. If a company installs a new system onto the network and does nothing more, all the vulnerabilities for that operating system and application are just sitting on the new server. Hackers will not have to look for new exploits because none of the old exploits have been corrected. So, new systems are loaded with the operating system, latest patches along with applications and their corresponding latest patches. This protects the system from know vulnerabilities. If a system is loaded with a non-supported vendor operating system, the system could never get to the point of warding of all known vulnerabilities. The vendor does not support or maintain the version that is being used. This creates an unnecessary risk for the servers and applications. By being at a software version that the vendor supports and maintains and loading the latest security patches for that version reduces the threat of old vulnerabilities affecting a server or application.

Another point is running on unsupported software from a vendor can lead to operational problems. If a problem arises because of a code issue or some anomaly that has never occurred before, the application or system is at jeopardy. The developer, database administrator, or system administrator will not be able to call the vendor to get a solution to the problem. This could severely impact revenue since transactions are what make GIAC Enterprises money and a server being down that deals with the transactions is not acceptable.

A policy must be put out that operating system and application software will be at supported vendor levels. Security patches will be installed as soon as they can be feasible installed after testing. If hardware will not support the new software, then new hardware must be considered when upgrading. Again policy and upper level management by off is the only way this will be accomplished.

Risk 3 – Change Control Policy

Change control policy is another area that needs to be addressed. Change control policy will encompass how development code is tested. It will cover how development code is moved into production. Changes to the system's operating system or any application parameters will be handled through change control. Hardware changes from replacement to hardware settings will be handled through change control. This policy covers all types of devices that are connected to the network and any application running on those devices.

Why be so detailed in change control? This information will allow for failing back if needed. Not all changes go as planned. If the change does not work, the old settings will need to be used. If a server or router or other piece of equipment is compromised, specific settings can be compared against what is stored with the change control database. This can also help identify that a system has been compromised.

Proper change control will mitigate the risk of shutting down a production server or segment of the network. The threat of applying software or hardware changes to a system or group of systems or even to the network devices could result in unpleasant situations. Change control cannot be overlooked.

Another risk that change control policy can help mitigate is licensing of software. Legal issues can become very expensive to combat in the legal system. This can financially hinder or ruin a company. Copyright laws and licensing of the software product needs to be examined to ensure that the software is valid legally on the system. This will ensure that there will not be any legal action that can be taken.

One last point is that plans and procedures do not always work out the way a person would like. These glitches will be documented within the change control process and help better plan for new changes. Hopefully, the same mistakes will not be made over and over.

The two questions that need to be asked are as follows. What are the crown jewels? How do these risks affect the crown jewels of the company?

Crown Jewels identified for risk

The core of the business is transactions that happen within the DB2 database in the mainframe. Any thing that would stop a transaction to or from the mainframe is catastrophic to our business model. The key is that the network must always be up. Our commodity is the transaction that takes place for a reservation. It is electronic. It is data only.

GIAC Enterprises greatest risk to the crown jewels is outdated software. The network and servers must be up all the time or revenue is lost. When software is not at a vendor-supported level, there is no maintenance or support given for the software. If a problem arises that will require that the vendor correct the issue with a code fix, this will not happen. The GIAC Enterprises developers' do not have access to the vendor proprietary code. There will not be any solution available to fix the problem and this will leave the operating system or application vulnerable or even worse not able to function correctly. The only recourse that might be available would be to upgrade immediately. This option is very dangerous since it will violate the "Change Control" policy. The software will not have the time to go through the development and testing phases that are needed.

Assignment 3 – Evaluate and Develop Security Policy

For this assignment I used the "Jackson Community College Computer Software Policy". It can be found at http://www.jccmi.edu/InfoTech/Documents/SoftwarePolicy.html. The full policy is listed in the Appendix under Jackson Community College Computer Software Policy".

The definition of a policy will outline specific requirements and rules that must be met.[16] The Jackson Community College Computer Software Policy deals with licensing, duplication, and distribution of software. The policy is being established to eliminate software copyright litigation. It focuses on the cost of litigation and penalties. The policy also points out that it is costly to trouble-shoot when there is a software conflict.

The purpose does an excellent job clearly identifying that all the computer software will be in compliance with copyright laws and licensing. The issue that is being address is not mentioned directly but can be interpreted. If all laws must be followed and all software must be licensed then it would be interpreted as being a legal issue. The purpose does not cover the cost or explain the extended trouble-shooting policy point.

There is background that is relevant to this policy. It explains the legal cost that can occur and other penalties for not following the policy. I think it was relevant to include this background into the policy.

The scope does explain the extent of the policy. The scope is for optimal service to all the clients maintaining cost. It covers the legal aspect of the policy with relationship to compliance. I think the part with the questions and the areas that a person can get more information should not be here. That part should be incorporated within the policy itself.

This policy is trying to address the risk of legal and software conflict issues. I see legal risk being if a software package is used illegally by not licensing correctly or ignoring copyright rules that a company could end up in the courts and lose. The courts could have a penalty assigned to the company that could be extremely expensive. This could effect the bottom line if a company has to fork out hundreds of thousands of dollars for each violation. It could cause financial hardship or even bankruptcy depending on the severity of the infraction. I feel this policy does a good job of clearly stating this legal issue.

This policy does address what steps should be taken for the legal risk. It covers how distribution of software outside and inside the organization will be handled. It covers how software can be copied. The policy covers the different types of available software.

This policy does cover which area should carry out the legal risk of software. The policy states that the IT area and all sites will not do copy or distribute software. The policy also states that users can use software within the software license agreement.

The software conflict portion of the policy is meant to address the costs associated with evaluating and testing software. I feel that this point in the policy is weak. I do not know what defines “extended trouble-shooting”. This part is open for much interpretation. I believe the concept is good because trouble-shooting software conflicts can be difficult. Th policy also does not address the issues of software that need to be retired within the policy directly. This point does relate to the risk that was stated about outdated software. I tie this together by looking at trying to add new software onto a system that is not supported by the vendor through maintenance or fixes. The new software is critical for production but this software cannot be loaded because of software conflicts. For example a new destructive code is out in the wild, this code will allow privilege rights on the affected system. The fix from the vendor will not correct the current version of software. The only fix is to upgrade. The questions that arise are “does the company have time to follow the proper testing and change control procedures?”, “does the upgrade affect other software applications?”. Either one of these scenarios could have a dramatic impact on the production server environment. It could lead to down time which affects the financial arena or worst yet it could affect the stability of the server or environment.

The steps to address software conflict are answered by stating that a reload will be done. It does mention that the user is responsible for a backup. The “what steps” and “who should carry them out” are answered in this bullet for the extended trouble-shooting issue. I feel that this takes care of individual user systems but not servers. This would be an issue with me. I would add in this that system administrators or data owners would need to backup the appropriate data first before loading new software. I would point the reader to the “Change Control Policy” because these issues would be covered there.

The responsibility seems to be listed within the scope of the policy. The Software Coordinator within the IT department has the responsibility for questions about policies. I do not see who can draft, approve, review, or modify this policy. It could be construed that the Software Coordinator would be the contact. Unfortunately, this policy does not make it clear on who will carry out specific policy directives.

The responsibility and action for each bullet point is missing. The first point is for no illegal software copying. There is no department authorized to check computer systems for illegal copies. There is no inventory or mechanism in place to check computers for illicit copies of software.

The second point is about illegal distribution. This point also states that there are penalties associated with this act. Again there is no department authorized to check computer systems for distributed software. There is not a department that will keep the inventory on what software is allowed for distribution or license count.

The third point is about public domain software. This point says that the software will be checked for viruses. It does not state who is responsible for checking for viruses. It does state when the virus checking will be accomplished.

The forth point is on shareware. It does not authorize a department to check if the software is allowed or licensed. It does not go in to detail on what constitutes the testing stage. This point does not say who will negotiate a site license.

The extended trouble-shooting point does not authorize a department to make the decision on when it becomes costly. There is no metric to support when this action would become costly.

New Server Security Policy [17] [18] [19]

The policy that was evaluated is broad in scope in the context of GIAC Enterprises. I have chosen to focus on a specific issue that incorporates the last point within the policy. It is dealing with extended trouble-shooting for software conflict. Under this point within the procedures is the retirement of software. The following "Server Policy" deals with both these issues.

Server Policy

Purpose

The purpose of this policy is to establish guidelines and standards for the configuration of internal server equipment that is owned by or operated for GIAC Enterprises. Effective implementation of this policy will minimize unauthorized

access to GIAC Enterprises proprietary information and technology. Another area is how are software conflicts minimized. Financial risk can increase if software conflicts exist.

Scope
This policy applies to server equipment owned by or operated for GIAC Enterprises, and to servers registered under any GIAC Enterprises owned internal network domain.

This policy is specifically for equipment on the internal GIAC Enterprises network. For secure configuration of equipment external to GIAC Enterprises on the DMZ, refer to the *Firewall Policy*.

Policy
Each internal server deployed at GIAC Enterprises will have an assigned system administration operational group with a point of contact that is responsible for the operating system administration. The Senior Operational Manager in charge of the data center will assign the system administration operational group.

Each internal server will have an assigned hardware operational group with a point of contact that is responsible for the hardware microcode of the server. The Senior Operational Manager in charge of the data center will assign the hardware operational group.

Any over-the-shelf, public domain, freeware or homegrown software application including but not limited to operating system, database, major or minor application, which resides on an internal server, will have an assigned application operational group with a point of contact. The Senior Development Manager or Senior Operational Manager in charge of the data center will assign the application operational group.

All vendor-supported software must be at a vendor-supported level for maintenance and fixes and be loaded with the latest vendor supplied security patches. Shareware, public domain, and custom software implementations must be used with discretion since there is no quick fix support for security issues that might arise. This will limit the exposure to software conflicts. A semi-annual audit of the software for all servers will be conducted by the GIAC Enterprises Audit organization. The Information Security team of GIAC Enterprises will conduct quarterly reviews of software versions. The system administration, hardware administration, and application administration groups will review monthly what software versions exist on the servers.

Approved server configuration guides must be established and maintained by each operational group (operating system, hardware, application), based on business needs and approved by GIAC Enterprises Information Security Manager. Operational groups should monitor configuration compliance and

implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by GIAC Enterprises Information Security Manager.

Each server must be registered within the "Distributed Systems Server Inventory". Information in the "Distributed Systems Server Inventory" must be kept up-to-date by the system administration, hardware administration, or application administration groups supply this information when new software, hardware, or modifications are done. Configuration changes for all servers must follow the appropriate change management policies and procedures found in the "Change Management Policy".

Establishing sessions with any server that utilizes the Intranet will use an encrypted technology for the session approved by the Information Security Manager.

Roles & Responsibilities

System Administration Operational Group:

- Responsible for the server operating system.
- Ensure vendor supports operating system version and the lasted security patches have been applied.
- Submit operating system information for the "Distributed Systems Server Inventory" per the guideline.
- Ensure that server network sessions are capable of encryption.

Hardware Operational Group:

- Responsible for the microcode that is installed on the hardware components of the server.
- Ensure vendor supports microcode and the lasted security patches have been applied.
- Submit hardware information for the "Distributed Systems Server Inventory" per the guideline.

Application Operational Group:

- Responsible for the application residing on the server.
- Ensure the vendor supports the application version and the lasted security patches have been applied.
- Submit application information for the "Distributed Systems Server Inventory" per the guideline.

Senior Development Manager

- Assign application operational group.
- New application will follow the "Procurement Policy" and a task assigned for this.

Senior Operational Manager in charge of the data center

- Assign system administration operational group
- Assign hardware operational group
- Assign application operational group
- New server or application will follow the "Procurement Policy" and a task assigned for this.

Distributed Systems Server Inventory Group:
- GIAC Enterprises Information Technology Senior Manager will determine the group who will be responsible for maintaining the inventory records.
- GIAC Enterprises Information Security organization will be given access to the "Distributed Systems Server Inventory" for quality assurance, audit capabilities, and research.
- Will keep the information within the "Distributed Systems Server Inventory" up-to-date with the minimum of the following information that positively identifies a server: name, location, type, operating system, maintenance release/patches, operational group(s), point of contact(s), and applications:

GIAC Enterprises Information Security
- Access to the "Distributed Systems Server Inventory".
- Check quality assurance of the "Distributed Systems Server Inventory" by performing security reviews.
- Perform security reviews for servers, hardware, and applications using information contained in the "Distributed Systems Server Inventory".
- Approve encryption technologies for use in the network and for servers.

GIAC Enterprises Audit Organization
- Audit servers, hardware, and applications to ensure versions are at supported levels and security patches are installed.

Appendix
Definitions
- DMZ: De-militarized Zone. A network segment external to the corporate production network.
- Server: For purposes of this policy, a Server is defined as an internal GIAC Enterprises Server.
- Hardware microcode: Software that resides on a hardware device to allow functionality. Also known as device drivers.
- Over-the-Shelf software: Software that can be purchased from a vendor.
- Homegrown software: Software written in-house.
- Public domain software: Software that is available freely. The software enhancements are supported by public input. This software has no copyrights.
- Shareware software (a.k.a. freeware): Software that requires a nominal fee. The software enhancements are supported by public input.

Guidelines
Distributed Systems Server Inventory Guideline:

- Server Name
- Server Physical Location
- Server Vendor
- Server Model
- Server Type
- Server Operating System Version
- Server Maintenance Release Level (if any)
- System Administration Operational Group
- System Administration Operational Group Point of Contact(s)
- Hardware Operational Group
- Hardware Operational Group Point of Contact(s)
- Hardware component Model
- Hardware component Type
- Hardware component microcode version
- Server Function
- Each Freeware, shareware, and custom software application will have the following information supplied.
  - Application Title
  - Application Vendor
  - Application Version
  - Application Maintenance Release Level (if any)
  - Application Operational Group
  - Application Operational Group Point of Contact(s)
  - Application Function

General Configuration Guidelines

- Operating System configuration should be in accordance with approved by GIAC Enterprises Information Security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.

- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Standards
Compliance

- Audits will be performed on a regular basis by authorized organizations within GIAC Enterprises.
- Audits will be managed by the internal audit group or by GIAC Enterprises Information Security, in accordance with the *Audit Policy*. GIAC Enterprises Information Security will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to by GIAC Enterprises Information Security, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

Procedures – Would be part of the policy structure.

Assignment 4 – Develop Security Procedures

System Administrator Organization Procedures:

- Will check monthly that the operating system version is at a vendor-supported level. This is for proper support.
  - Accomplish by logging on to server and using native commands to check operating system level.

  - Log on to the vendor web site and compare what versions of software are supported and what level are the servers.
  - If an update is needed, follow the "Change Control Policy" for implementation.

- Will check at least weekly that the operating system has the latest security patches. This is for proper security.
  - Accomplish by logging on to server and using native commands to check security patch levels.
  - Log on to the vendor web site and compare what patch levels of security patches are available and what level are the servers at.
  - If a new patch is needed, follow the "Change Control Policy" for implementation.

- Any new server will be assigned a system administration operational group from the task that the "Procurement Policy" assigned to the Senior Operational Manager in charge of the data center.

- For a new server or modification to a server, the following information must be submitted to the Distributed Systems Server Inventory:
  - Server Name
  - Server Physical Location
  - Server Vendor
  - Server Model
  - Server Type
  - Server Operating System Version
  - Server Maintenance Release Level (if any)
  - System Administration Operational Group
  - System Administration Operational Group Point of Contact(s)
  - Server Function

Note: This will give greater control on what is out in the environment and make it easier to ensure the proper security checks are in place.

- If there is an application that this area supports then the following information needs to be given:

- Any new application will be assigned a system administration operational group from the task that the "Procurement Policy" assigned to the Senior Operational Manager in charge of the data center or the Senior Development Manager depending on how the application is procured.

- Each Freeware, shareware, and custom software application will have the following information supplied.
  - Application Title

- Application Vendor
- Application Version
- Application Maintenance Release Level (if any)
- Application Operational Group
- Application Operational Group Point of Contact(s)
- Application Function

- Before any server is connected to the network, ensure that encryption is used for communications to/from the server.
  - Check with the GIAC Enterprises Information Security organization to see what products are acceptable.
  - If the product chosen is not on the acceptable list because it is new, submit a request to GIAC Enterprises Information Security organization to evaluate. This server will have to wait until the request is reviewed and accepted by the GIAC Enterprises Information Security Manager before it is allowed onto the network.

- Semi-annual audits will be performed by the GIAC Enterprises Audit organization. They will check the server operating systems and applications for proper versions and security fixes. The audits will also check the Distributed Systems Security Inventory against what is found within the environment for accuracy.

Appendix

Jackson Community College Computer Software Policy [20]
Located at http://www.jccmi.edu/InfoTech/Documents/SoftwarePolicy.html

Table of Contents

Jackson Community College Software Policy
Software policies and procedures are designed to provide optimal service to all clients (students and employees) in a cost-effective manner and in compliance with all regulations and laws. If you have questions concerning a particular policy

or process, please review JCC's Responsible Use Policy or **contact the Software Coordinator** in Information Technology (IT).
Jackson Community College will respect all computer software copyrights and adhere to the terms of all software licenses to which it is a party.
§ No software available through the Information Technology department or any of its college sites may be copied unless permission to do so is explicitly stated on the disk or the software program. Unauthorized duplication of software may be grounds for termination of access, disciplinary review, expulsion, termination of employment, and/or civil/criminal penalties under the United States Copyright Act.
§ No software available through the Information Technology department or any of its college sites may be distributed to clients, customers, contractors, students, employees, and others. Users may use software on local area networks or on multiple machines only in accordance with license agreements. Unauthorized distribution of software may be grounds for termination of access, disciplinary review, expulsion, termination of employment, and/or civil/criminal penalties under the United States Copyright Act.
§ Public domain software may be copied and shared because it is not subject to any copyright restriction. The software author has decided to provide this software to the public free of charge. Public domain software must be checked for viruses prior to copying or using.
§ Shareware is copyrighted software that the developer encourages you to use and then purchase. Shareware may not be used beyond the testing stage without being purchased. Site licenses can be negotiated for shareware.
§ Extended trouble-shooting for software conflict is costly to JCC. Standard procedure for extended software conflict includes reloading a computer with a standard load. Backup of computer files **prior to the reload process** is the responsibility of the user. The Solution Center is available to help users understand and complete backup procedure.
According to the United States Copyright Act, illegal reproduction of software is subject to civil damages of as much as US$100,000 per title infringed, and criminal penalties, including fines of as much as US$250,000 per title infringed and imprisonment of up to five years.
Back To Top
Jackson Community College Software Procedure

software purchase: cycle

JCC purchases software three times each year. The software order is compiled by the Information Technology Software Coordinator and sent to purchasing the second week of each semester. This applies to computer classroom and computer lab software. Purchase requests may be turned in at any time during the cycle. Purchase requests turned in after the deadline will be held for the next purchase cycle.

Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July
	Software				Software				Software		

	ordered				ordered				ordered		

Installation of standard software ordered in a purchase cycle is guaranteed by the beginning of the next semester with the following exceptions:
§ Vendor out-of-stock
§ Vendor late shipment
§ Technical situation beyond control of IT personnel
Each of these may impact testing and release of software for classroom use. Please see testing and release of software for classroom use below.
Software is approved by the Software Coordinator in Information Technology to ensure software compliance, compatibility, and licensing. Purchase orders sent directly to Purchasing will be returned to the Software Coordinator for approval. A complete record of all software is required to accommodate auditing by national and international software agencies and to ensure the support and upgrade of software. Software acquired will first be delivered to the Software Coordinator in order to complete required paperwork. The Software Coordinator will complete registration, inventory, and media backup. The Software Coordinator will return registration information to the software publisher. Software will be registered in the name of the organization. Non-standard, but approved, software will be delivered to the client for installation.
Software not purchased through this process is considered unsupported. However, IT encourages employees to experiment with new software (downloading demo versions and trying them out) for the following reasons:
§ Useful software for institutional and office purposes will be found
§ If a software problem occurs with a computer with non-standard software installed, the reload process allows for quick restoration of service
NOTE: If you have installed non-standard software and encounter problems with your computer, follow this procedure:
1. Call the Solution Center, extension 8639
2. Notify the Solution Center that you have installed non-standard software and are encountering problems
3. Schedule a time for a reload

testing and release of software for classroom use

§ Software must be technically tested by Information Technology prior to deployment.
§ The Software Coordinator will notify all employees through e-mail when software is available for testing.
§ An instructor in an instructional setting must test software with the standard load http://www.jccmi.edu/InfoTech/Software/StandardLoad.htmlto ensure that the software load will serve instructional needs.
§ Instructors are urged to contact the Software Coordinator or the Solution Center prior to start-up of classes not only when a problem exists but also when testing is complete and no problem exists.

If software is ordered on time but received late due to software company difficulties, then extended effort from Information Technology and from faculty may be required to meet start-up deadline for classes.

software purchase: capacity

Sufficient licenses need to be purchased to accommodate:
§ Course instructor(s)
§ Course offering in a computer classroom
§ Student access in an open computer lab unless open computer lab access is deemed unnecessary by the program coordinator.
The Software Coordinator determines number of licenses required.
Information Technology is developing the process for software access monitored by metering software to accommodate increased scheduling flexibility of computer classrooms and labs. Metering, in partial implementation, will begin Fall 2000.

software purchase: cost

Information Technology purchases standard software, e.g., Microsoft Office, NetWare, First Class, Windows, etc.. Adequate processes for the purchase of specialty software necessary for instructional and administrative programs, e.g., Photoshop, Illustrator, PageMaker, Alchemy, Razor's Edge, CEO, are being developed.
Software purchased by Information Technology
Specialty software used at JCC

flexibility and late requests

Information Technology will make every reasonable effort to remain flexible in process for the benefit of instruction and administration unless requested flexibility negatively impacts mission critical operations. In particular, Information Technology will remain flexible in process when dealing with software company difficulties (release date changes, out-of-stock notices) and when dealing with instructional need to offer a course when the need to offer that course could not have been reasonably foreseen (e.g., technological advances).
Courses requiring software that was not planned for and the need could have been foreseen will be delayed until the following reasonable purchase cycle/semester.

fiscal responsibility

Dividing software cost by billing contacts will develop a measure of cost effectiveness. More detailed measures will be developed in the future.
Information Technology will compile this information two weeks after each semester start. The information will be distributed to Instructional Work Groups, the Dean of Faculty, the Vice President for Instruction, and the Business Office for their use in decision making.

retirement of software

The following criteria will be used when determining if software needs to be retired:

§ Does the software run with current Operating System without conflict?
§ Does the software run with current Operating System and without conflict with other software?
§ Does the software run with current Operating System and without excessive maintenance?
§ Has the software been determined cost effective? Please see Fiscal Responsibility above.
§ Is the software sufficient for task and does it provide optimum learning experience for students?
NOTE: If software is deemed necessary to instructional and/or administrative needs, then an appropriate replacement needs to be acquired prior to software retirement.

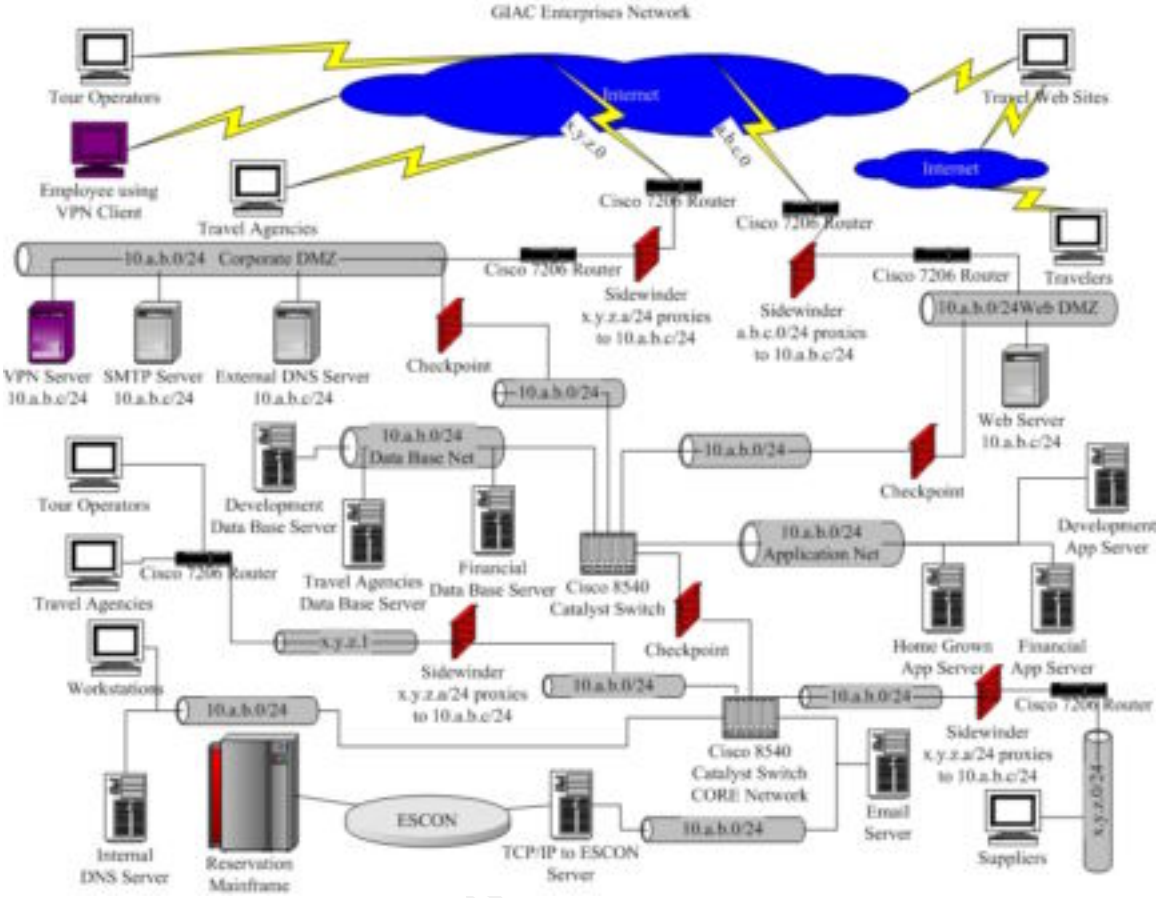
software upgrades: lab and classroom

Currently, Information Technology Education (ITE) instructional needs determine the timing of standard software upgrades for JCC's computer labs and classrooms. ITE instructional needs are determined by the student/customer need/desire to have instruction with current software.

web access to software information

Information Technology provides an up-to-date web page detailing software information for JCC:
http://www.jccmi.edu/InfoTech/
Back To Top

Network Diagram



References

Used Author's Company Web page as framework for this paper. Sanitized and modified the way web page information is stated.

"eTrust CA-ACF2 Security for z/OS & OS/390 Release 6.4". http://www3.ca.com/Solutions/Collateral.asp?ID=792&PID=147(9-25-02).

"Trust CA-ACF2 Security for DB2". http://www3.ca.com/Solutions/Product.asp?ID=146(9-25-02).

"Cisco 7200 Series Routers Product Overview". http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_chapter09186a008007db1c.html#36513(9-12-02).

"Cisco Catalyst 8500 Series Multiservice Switch Routers". http://www.cisco.com/en/US/products/hw/switches/ps718/products_configuration_guide_chapter09186a00800ea08e.html(9-13-02).

"www.securecomputing.com/pdf/86-0936782-B.pdf". http:// www.securecomputing.com/pdf/86-0936782-B.pdf(10-11-02).

"Firewall Security (Sidewinder Security)". http://www.securecomputing.com/index.cfm?sKey=1023(9-9-02).

"FireWall-1 Home". http://www.checkpoint.com/products/protect/firewall-1.html(9-6-02).

"Exchange 2000 product Overview". http://www.microsoft.com/exchange/evaluation/overview/default.asp(9-17-02).

"Sun ONE Web Server – Overview". http://wwws.sun.com/software/products/web_srvr/home_web_srvr.html(10-11-02).

"Windows 2000 Resource Kits". http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/intwork/inbe_vpn_naxe.asp(9-18-02).

"Symantec AntiVirus Enterprise Edition". http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=86&PID=12763555&EID=0(10-11-02)

"Top 10 Reasons to Move to ISA Server" http://www.microsoft.com/isaserver/howtobuy/upgrade.asp(9-18-02).

"IBM Installation Services for WebSphere Application server – Advanced Edition". http://www-1.ibm.com/services/its/us/ss-websphere.html(10-11-02).

"CERT Security Improvement Modules".Source http://www.cert.org/security-improvement/(8-1-02thru10-10-02).

"Software Policy". Note: Used this policy for Assignment 3 "Evaluate and Develop Security Policy". http://www.jccmi.edu/InfoTech/Documents/SoftwarePolicy.html(10-13-02)

Earnst and Young Security Policy and Standards project done for author's company.

SANs Information Security Officer Training course.

EndNotes

[1] Source is from author's company. The information has been sanitized, changed the format and numbers. Content is somewhat the same.
[2] "eTrust CA-ACF2 Security for z/OS & OS/390 Release 6.4" http://www3.ca.com/Solutions/Collateral.asp?ID=792&PID=147(9-25-02).
[3] "Trust CA-ACF2 Security for DB2". http://www3.ca.com/Solutions/Product.asp?ID=146(9-25-02).
[4] "Cisco 7200 Series Routers Product Overview". http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_chapter09186a008007db1c.html#36513(9-12-02).
[5] "Cisco 7200 Series Routers Product Overview". http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_chapter09186a008007db1c.html#36513
[6] "Cisco Catalyst 8500 Series Multiservice Switch Routers". http://www.cisco.com/en/US/products/hw/switches/ps718/products_configuration_guide_chapter09186a00800ea08e.html(9-13-02).
[7] "www.securecomputing.com/pdf/86-0936782-B.pdf". http://www.securecomputing.com/pdf/86-0936782-B.pdf(10-11-02).
[8] "Firewall Security (Sidewinder Security)". http://www.securecomputing.com/index.cfm?sKey=1023(9-9-02).
[9] "FireWall-1 Home". http://www.checkpoint.com/products/protect/firewall-1.html(9-6-02).
[10] "Exchange 2000 product Overview". http://www.microsoft.com/exchange/evaluation/overview/default.asp(9-17-02)
[11] "Windows 2000 Resource Kits". http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/intwork/inbe_vpn_naxe.asp(9-18-02).
[12] "Top 10 Reasons to Move to ISA Server". http://www.microsoft.com/isaserver/howtobuy/upgrade.asp(9-18-02).
[13] "Sun ONE Web Server – Overview". http://wwws.sun.com/software/products/web_srvr/home_web_srvr.html(10-11-02).
[14]"Symantec AntiVirus Enterprise Edition". http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=86&PID=12763555&EID=0(10-11-02)
[15] "IBM Installation Services for WebSphere Application server – Advanced Edition". http://www-1.ibm.com/services/its/us/ss-websphere.html(10-11-02).
[16] Source is from the SANS web class GISO. "Track 9 SANS Information Security Officer Training".
[17] "CERT Security Improvement Modules".Source http://www.cert.org/security-improvement/(8-1-02thru10-10-02).
[18]Source Earnst and Young Security Policy and Standards project done for author's company.

[19] Source is from author taking SANs Information Security Officer Training course.
[20] "Software Policy". http://www.jccmi.edu/InfoTech/Documents/SoftwarePolicy.html(10-13-02)