Global Information Assurance Certification Paper

Information Security for GIAC Enterprises

GIAC Information Security Officer

Practical Assignment
Version 1.2

Kelly Cook

Friday, January 10, 2003

Table of Contents

ABSTRACT **1**

ASSIGNMENT 1: DESCRIPTION OF GIAC ENTERPRISES **2**

GIAC Enterprises Company Mission 2
Company Description 2
IT Security Overview 3
IT Infrastructure 4
Network Layout *5*
Network Infrastructure *7*
Physical Security 8
Other Security Measures 8
Business Operations 9
Business Process Overview *9*
Data Display, Transmission, and Access *10*

ASSIGNMENT 2: IDENTIFY RISKS **11**

Areas of Risk 11
Risk 1: Unauthorized access to GIAC Enterprises' IT assets (network, systems, and databases). *11*
Risk 2: Virus or other malicious software attack to the GIAC Enterprises network. *15*
Risk 3: Unauthorized System and/or Database Changes *18*

ASSIGNMENT 3: EVALUATE AND DEVELOP SECURITY POLICY **21**

GIAC Enterprises Current Anti-Virus Policy 21
Critique of Original Policy and Revised Anti-Virus Policy 22
GIAC Enterprises Revised Anti-Virus Policy 24

ASSIGNMENT 4: ANTI-VIRUS SOFTWARE INSTALLATION PROCEDURES **27**

APPENDIX I: NETWORK DIAGRAM **30**

REFERENCES **31**

Abstract

GIAC Enterprises provides medical billing services to physicians and group practices. GIAC Enterprises, located in Dallas, Texas, has a total staff of 125 employees. Information Security measures and policies are the foundation for GIAC Enterprises. Especially with the bulk of the company's operations interacting with the Internet, a myriad of vulnerabilities and threats are ever-present. Therefore, GIAC Enterprises follows the philosophy that a combination of security strategies and tools must be deployed. IT Security at GIAC consists of the balance between three core components of the business: staff, technology, and the business operations.

This document details GIAC Enterprises' IT infrastructure, business operations, areas of security risk, and steps taken to mitigate the identified security risks. In addition, the paper provides a critique and evaluation of how a current anti-virus policy should be rewritten for greater clarity and effectiveness. This document includes a network diagram with all major key components identified and details how the company's network is segmented into a public segment (DMZ), a protected segment, and a secured segment.

This document is a product of the author's professional work experience and contributions to his organization as well as external research materials and papers. References have been cited in the text as well as in the References section at the end of the paper. In addition, all material has been sanitized and fictionalized to prevent exposure of any proprietary information.

Assignment 1: Description of GIAC Enterprises

GIAC Enterprises Company Mission

The mission of GIAC Enterprises is to provide healthcare clients with superior medical billing services.

Company Description

GIAC Enterprises provides medical billing services to physicians and group practices. In the medical field today, healthcare providers face the challenge of proficiently managing a business in addition to providing patients with healthcare services. Therefore, many practices subscribe to GIAC Enterprises to handle medical billing services that are compliant with the Office of Inspector General (OIG) Third Party Billing Guidelines and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The company transmits claims electronically to Medicare, Medicaid, and hundreds of other insurance companies, and bills the patients for the remaining balance. In addition, paper claims are also submitted for those cases where electronic claims are not accepted. Once healthcare clients receive insurance payments for services rendered, GIAC Enterprises creates patient statements for any remaining balances, follows up with outstanding balances, and provides customer service for any billing questions from patients. In addition, physicians and group practices can access their practice profile online to receive various practice management reports.

GIAC Enterprises, located in Dallas, Texas, has a total staff of 125 employees. The company is composed of several smaller departments, each performing a specific function. The numerical distribution for company employees is as follows:

Senior Management: 4 Employees

This group is composed of GIAC Enterprises' President, Vice President, Managing Director, and Chief Information Officer.

GIAC Internal Operations Division:

- **ITD Department**: 25 Employees
  Provides and manages the data processing related to the claims processing and billing services for our customers through the utilization of existing and new information technology. ITD implements and supports technologies and processes that will increase service to customers and enhance staff productivity. In addition, the ITD develops, maintains, and supports the GIAC Enterprises internal network and company systems.

- **Financial Management Department**: 31 Employees
  - **Accounting and Accounts Payables Team:** Manages annual audit, general ledger system, bank reconciliation process, special budgets, debt payment and tracking. In addition, team handles:
    - Revenue collection
    - Processes bi-weekly payroll
    - Accounts for fixed assets
    - Processes accounts payable checks
  - **Accounts Receivables Team:** Issues monthly billings for materials sold or services rendered to our customers. In addition, this team follows up on delinquent payments.

- **Sales and Marketing Department**: 5 Employees
  Introduces GIAC Enterprises and its services to healthcare markets to find new customers and capture the medical billing services market share.

- **Purchasing Department**: 5 Employees
  Supports GIAC Enterprises with the identification, selection and acquisition of required materials and services.

GIAC Client Services Division:

Customer Liaison Department: 40 Employees
Manages and interacts with our healthcare provider customers to manage and answer any questions on their accounts and services with us.

Patient Billing Inquiry Department: 15 Employees
Manages any patient inquiries regarding their insurance claims or billing statements.

IT Security Overview

Information Security measures and policies are the foundation for GIAC Enterprises. Especially with the bulk of the company's operations interacting with the Internet, a myriad of vulnerabilities and threats are ever-present. Therefore, GIAC Enterprises follows the philosophy that a combination of security strategies and tools must be deployed.

IT Security at GIAC consists of the balance between three core components of the business: staff, technology, and the business operations.

Staff: GIAC's senior IT management (i.e, CIO, other IT managers) have committed to understanding the company's primary threats and risks. As such, various information security policies and procedures are consistently communicated and carried out. In addition, appropriate roles and responsibilities have been assigned

to staff and necessary training is provided. Furthermore, physical security of the company's premises is established to protect both staff and the company's critical information resources.
Technology: GIAC's technology resources are deployed to ensure optimal coverage for the defense-in-depth strategy of IT security at the company. Primary measures include the following implementations:

1. Network boundaries are protected by firewalls and intrusion detection tools.
2. Nested firewalls paired with intrusion detection are deployed within the network to provide greater layered defense.
3. Data transmission over the network is done so in a manner that protects confidentiality and integrity of data through use of encryption and security mechanisms.
4. Regular system backups are performed, both to a mirrored hard drive and to tape media. In addition, backup tapes are sent offsite for storage.

Operations: GIAC's activities on a day-to-day basis incorporate several processes to maintain the company's IT security. Primary measures include the following activities:

1. System security assessments are performed on a periodic basis to evaluate the company's current vulnerabilities and threats.
2. Security policies are consistently updated as needed and made available to all.
3. Proper security patches and virus updates are applied.
4. User access lists are kept current and up-to-date.
5. Network attacks and emergencies are handled in an organized and efficient manner.
6. Business recovery and reconstitution are implemented effectively when needed (United States of America National Security Agency 2-3).

IT Infrastructure

GIAC Enterprises' network consists of public, protected, and secured subnets. The company's TCP/IP network consists of the public and protected subnet segments, while the secured subnet (only accessible remotely via a VPN) consists of the company's user network and internal databases network.

Entrance from the Internet into the GIAC network follows the following flow: the ISP Router, the Cisco border router, and then the Checkpoint FW-1 firewall. Within each subnet of the network resides an IDS tool (ISS RealSecure) to monitor traffic for any suspicious or attack events In addition, the Check Point firewall sits between the border router and any of the three subnets. In addition, nested firewalls at the entrance of both the protected and secured subnets for added security.

In addition, to protect the company for viruses, anti-virus software is installed. All of the user workstations, servers, and remote users' computers use McAfee VirusScan, while the public mail relay server and the internal mail server use GroupShield.

Network Layout (Please refer to Appendix I: Network Diagram.) The GIAC Enterprises network is divided into separate subnets to ensure the optimization of security and performance measures. Each subnet consists of various components.	
Public Subnet	• **Web Server**: Displays the corporate Internet site for the public. • **E-Mail Server**: Provides E-Mail services for company employees. • **DNS Server**: Provides translation of domain name to IP address. • **IDS**: ISS RealSecure is used as the intrusion detection tool. The focus here is on general traffic load, the DNS server, the mail relay server, and the web server. • **VPN Gateway**: This is the VPN device for the company's remote access function.
Protected Subnet	• **IDS**: ISS RealSecure is used as the intrusion detection tool. The focus here is on monitoring for suspicious and malicious traffic to and/or from the Customer Server, the Partner Server, the Suppliers Server, the Syslog Server, and the RSA Ace

	Server. • **Supplier's Server**: Current suppliers of GIAC Enterprises can access the protected segment of the site that concerns their business with GIAC. • **Customer Server**: Current customers of GIAC Enterprises can access the protected segment of the site that concerns their practice information supplied from GIAC. • **Partner Server**: Current partners of GIAC Enterprises can access the protected segment of the site that concerns information about their partnership with GIAC. • **RSA Ace Server**: The Ace Server provides two-factor authentication services for all of the servers in the network spanning all three subnets (Krychiw "The Secure ID Solution"). • **Syslog Server**: The Syslog Server serves as the central repository for the logs from all of the servers on the entire network (public, protected, secured subnets). This server houses a copy of each server's log and therefore serves as a backup in the event that a server loses its log, and it is helpful for intrusion and fault detection analysis (CyberGuard 4-5).
Secured Subnets	***User's Network:*** • **Staff Workstations**: GIAC Staff desktops and laptops.

	• **IDS**: ISS RealSecure is used as the intrusion detection tool. The focus here is on monitoring for suspicious and malicious traffic to and/or from the staff workstations and the internal mail server. • **Internal Mail Server**: Handles company internal mail functions. ***Internal Database Servers Network:*** • **IDS**: ISS RealSecure is used as the intrusion detection tool. The focus here is on monitoring for suspicious and malicious traffic to and/or from the company's critical information databases. • **Critical Databases** (Production, Test, Development, etc.)

Network Infrastructure

The network infrastructure is composed of various components. The key components include the following items.

Network Component	Component Brand and Version
Border Router	Cisco 3640 with IOS 12.2 (2)T
Primary and Secondary Firewalls	Check Point Firewall FW1
Nested Intranet Firewalls	Cisco Secure PIX 525
VPN Gateway	Cisco Concentrator 3000 Gateway
Intrusion Detection System	ISS RealSecure Network Sensor

Physical Security

The physical security of the GIAC Enterprises' data center is an integral key to protecting the company's data.

The data center is maglock protected and secured. The center has two security cameras that are monitored by security staff. Only data center personnel can access the room. Personnel have an access card to enter the room, and wear picture ID badges. Guests must have special badges and be escorted. All guests must enter from the main door and sign in with the receptionist and wait for the authorized escort.

The access to servers and/or workstations is secured against unwanted and unauthorized access. Permission to be issued electronic card key access to the data center must come from the authorized official. Permission is granted on an as-needed basis. The floor in the server room is raised. There is also a locked door to the server room, and both employees and guests who wish to enter the server room must be wearing visible name tags.

In terms of protection against the possibility of a fire, the following characteristics are present in respect to the IT premises:

- fire door to the server room
- fire detectors inside the server room
- fire extinguishers
- fire detectors outside the server room
- test of fire equipment

Furthermore, there is air condition present in the server room and the room is a climate-controlled environment. The servers are also placed on a raised platform, and there are no windows present in the server room. An Uninterruptible Power Supply (UPS)-system is present, and there are annual tests of the UPS-system including the full shut off of power. In addition, the company has a well-communicated and adopted emergency evacuation plan.

The modems and the main distributing frame are locked and securely stored in the data center. The IT equipment are all labeled accordingly.

Other Security Measures

The company has a general information security policy that applies for the whole company. GIAC's Information Security Policy's purpose is to protect information that is critical to business operations, and to ensure information resource confidentiality, security and integrity. It is made accessible by the organization to employees through a link at the company's Intranet web address.

GIAC has a separate Internet policy that is different from the above mentioned policy. The Internet and E-Mail Usage Policy defines the proper use of electronic mail and internet services for employees with the company. In addition, password policy, remote access (VPN) policies are also communicated and posted on the company web site. In addition, all employees are required to sign and date a non-disclosure agreement agreeing to maintain confidentiality of GIAC's information.

Business Operations

Business Process Overview

GIAC Enterprises business operations involve data transmission and receipt via the Internet. Overall, the medical billing services industry is a competitive and challenging field. Medical billing professionals must accurately file claims in accordance with the current coding rules and regulations. GIAC customers are individual physician practices and group practices.

Medical practices submit their superbills electronically over the Internet or send them via overnight courier or snail mail. Each practice that is a registered customer of GIAC Enterprises can select either only electronic claims submission services or full service billing services (transmit electronic claims, submit paper claims when necessary, print and mail patient statements, follow-up on claims, respond to patient calls, produce practice production reports). The fee to the customer is based on whether the practice is registered for the electronic claims submission services ($3.25 - $5.50 per claim) or the full service billing services (usually between 7 to 10 percent of each month's collections).

The practice can login to GIAC's web site. Each practice is assigned a User Name. Then, each practice selects its own password (according to the password rules distributed by GIAC). The website allows the practice to view its practice-specific information securely through VeriSign's 40-bit SSL encryption. In addition, each practice can submit its electronic superbills at the close of business each day in a batch process via the Internet through VeriSign's 128-bit SSL encryption to ensure confidentiality. Accuracy of data entered for each superbill is the responsibility of the customer, while our online application verifies each field for correct field type and length. SSL encryption protects the practice's confidential information from hackers and other interceptions (VeriSign "What is the difference between a VeriSign 40-bit SSL Certificate and a VeriSign 128-but Global Server ID").

In addition to our customers, our partners and suppliers also log into the GIAC website in order to access information specific to their relationship with us. GIAC Enterprises defines a distinct relationship between us and our suppliers versus our partners. We view suppliers as vendors who rarely participate or are affected in

the success and efficiency of our business and our customer's satisfaction, but rather provide, or supply, us with needed goods for our operations. On the other hand, GIAC views its partners as companies and organizations who provide us with a service with the mutual interest in our success for a particular aspect of our operations, and who are willing to be held accountable for managing and measuring our success.

Companies that wish to be considered as a GIAC Enterprises supplier (ex. stationary, IT equipment, communications, etc.) and interested in receiving Requests For Information (RFI's) and Requests for Proposals (RFP's) must register and receive an approval by GIAC Enterprises. The process of approval includes the following steps:

1. The supplier selects "Become a Supplier" button on the GIAC Enterprises website and proceeds to fill out and submit their information.
2. The GIAC Procurement Office reviews the potential supplier's data and decides whether or not the company can be accepted as an approved supplier.
3. Approved suppliers will receive log-in information in a physical letter.
4. Once a suppler is an approved supplier to GIAC Enterprises, they are able to log into the system. During the initial login session, the supplier is prompted to confirm the company data and to establish a company profile.
5. The supplier is now set-up to receive RFI's and RFP's and to participate in competitive tenders GIAC Enterprises.

Approved suppliers login to the GIAC Enterprises website to view RFI's and RFP's. In addition, they can respond with the requested information and/or quotation for a particular RFI and RFP and await online responses by our procurement office.

Similarly, companies and organizations who wish to be considered a GIAC Enterprises partner select the "Become a Partner" button on the GIAC Enterprises website and await acceptance and confirmation into our partners program. Partners can access the website to view current initiatives they are involved in with us and be notified of any system, policy, and procedure changes for initiatives that involve them. In addition, partners can propose and submit any additional initiatives they feel would be beneficial to us.

Both suppliers and partners are able to view their information in 40-bit SSL encryption and submit information with the 128-bit encryption to ensure confidentiality.

Data Display, Transmission, and Access

GIAC Enterprises both accepts and displays data on its website in a secure manner. Each practice registers itself online with all pertinent practice information and uploads its patient and insurance information. Also, the close of business superbills are submitted via the website. Such data transmission retains its integrity and reliability through the use of VeriSign's 128-bit SSL. Each practice can access its own pre-designed financial reports, insurance payments, cash,

claims reports, and write-off reports. Also, various statistical reports based on historical billing data can be created. All of these reports are accessible via the Web from the system's database in a "read-only" format that prevents any information corruption. The web site displays such information via VeriSign's 40-bit SSL encryption.

GIAC employees can access company E-mail, company Intranet, and internal database servers via the Cisco 3000 Concentrator Virtual Private Network (VPN) and the Cisco VPN Client (Easy VPN). The VPN uses encryption, tunneling, and various security measures to ensure that authorized company users can access GIAC Enterprises' network in a manner that is safe and reliable.

Assignment 2: Identify Risks

Areas of Risk

GIAC Enterprises manages and processes various medical practices' information that is contained in a medical superbill. Such information as patient personal information (name, address, telephone number, etc.), billing information, and insurance information are listed. In addition, practice-provided information (each practice's billing codes, rules, etc.) are also housed within GIAC's information systems to enable each practice to access its specific practice and statistical reports.

Therefore, such patient information and practice-specific information are the "crown jewels" of GIAC Enterprises'. Therefore, data accuracy, correct use of information, and prevention of information leakage must be of utmost importance to GIAC Enterprises.

Three primary risks that have been identified as being present include the following items:

1. Unauthorized access to the GIAC Enterprises' IT assets (network, systems, and databases).
2. Virus or other malicious software attack to the GIAC Enterprises' network.
3. Unauthorized system and/or database changes.

Risk 1: Unauthorized access to GIAC Enterprises' IT assets (network, systems, and databases).

- **Description of the Risk**

IT assets can be significantly damaged by unknown and unauthorized individuals. The threat of unauthorized access results in loss, disclosure, modification, or

destruction of a company's critical information resources, leading to business disruption and emergency. Such activity can cause GIAC Enterprises to face serious adverse economic or legal consequences. In addition, the individual attempting such unauthorized access can face serious disciplinary action and personal consequence as well.

The likelihood, or risk, of unauthorized access occurring is high because there are several high threats and a high level of vulnerability. Through this security risk assessment, GIAC Enterprises' is most vulnerable to unauthorized access attempts primarily because of a lack of documented and enforced password policies and a lack of a formal monitoring of security logs to identify and address potential intrusions or inappropriate use of data assets.

- **Justification for Company Concern of This Risk**

The nature of GIAC's business operations allows for the risk of unauthorized access to be prevalent in various entry points to the company's IT assets. First,

GIAC's business operations significantly involve the use of the Internet. An analysis of the security logs during this assessment revealed that there are a high number of unauthorized malicious access attempts that arrive via the Internet. Such attempts serve as a constant reminder to GIAC Enterprises that there is a high risk and probability of a successful malicious access attempt if the company is vulnerable by not being aware of the latest security technologies and best practices encompassing GIAC's people, processes, and technology. These access attempts that arrive via the Internet are of major concern to GIAC Enterprises for the following reasons:

1.) **GIAC Website Defacement and DNS Spoofing** – If a hacker or unauthorized internal employee gains access to the site files stored on the GIAC web server, he/she can alter the files in any way. A defacement of the company's website would be detrimental because a malicious unauthorized individual could publish untrue and harmful information regarding the company or erase crucial pages and links. A disruption of business processes and operations can occur if the malicious individual manages to eliminate or disable partners, suppliers, and especially customers (the hospitals and doctor's offices) from accessing their information via their login screen. For example, the customers would not be able to post their super bills or access their billing summaries and reports, which would in turn disrupt their business operations.

Another threat is if DNS spoofing occurs. A DNS spoof can occur if the hacker is able to alter the DNS entry on GIAC's server to redirect the browser to an alternate site that appears visually the same but transmits data to the hacker's destination. This is of great concern to GIAC Enterprises because any redirection of patient and practice information that customers post would result in the transmission of confidential data to malicious individuals.

2.) **Access to GIAC Databases and Systems -** The company's "crown jewels"

(patient information and customer (healthcare practice-specific information) reside on the internal GIAC databases. Unauthorized individuals, either within the company (knowingly or unknowingly) or external hackers that could access the databases would have access and could potentially copy or alter patient personal information, insurance information, or our customers' practice-confidential information and statistics. Any alteration to data would compromise the integrity of the data submitted for claims and billing and any disclosure of data (patient/practice information) would result in a breach of confidentiality for GIAC Enterprises. Especially with the Office of Inspector General (OIG) Third Party Billing Guidelines and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations that GIAC Enterprises must follow, any compromise to the integrity of the data stored in its systems and databases would result in a tarnished company reputation, loss of business, and serious legal consequences.

- **Possible Consequences from an Exploitation of This Risk**

Both hackers and internal employees with malicious intent constantly try to enter company networks and protected areas through exploitation of known security weaknesses. If the network is not well planned and secured, it is easily subject to penetration by intruders. In addition, inadequate security sometimes results in unintentional changes by internal employees with no malicious intent. However, after this security assessment, GIAC Enterprises is satisfied with the layout and security mechanisms in place in the network architecture. Nonetheless, successful access to the network by such intruders, resulting in corruption of the network and that data that is contained within it, can still occur since GIAC Enterprises lacks documented and enforced password policies and a formal process of monitoring security logs to identify and address potential intrusions or inappropriate use of data assets.

Since GIAC Enterprises possesses two main vulnerabilities, a lack of a documented and enforced password policy and a formal process for monitoring security logs, there is a high possibility that unauthorized access could easily occur and damage could go undetected or be irreversible. Corruption of the IT assets would lead to major business disruption and bring to a halt of regular business operations. In addition, unnecessary expenditures will be incurred by GIAC Enterprises to recover or replace damaged or deleted files. The network and data corruption would affect business continuity resulting in loss of business revenue. Frequent inaccuracies in data may cause the company to lose the respect of customers, partners, and suppliers.

- **Risk Mitigating Steps**

GIAC Enterprises has taken several steps and measures to mitigate the risk of unauthorized access to GIAC Enterprises' IT assets. The company feels that the current network architecture and design promote a secure environment. However, this security risk assessment has also highlighted several opportunities for

improvement.

Currently, GIAC has the following risk mitigating **steps in place**:

- The company's network has been segmented into public, protected, and secured subnets. When public visitors enter the GIAC web site, they are able to view the informational content, such as the background about the company, services provided, and contact information. On the other hand, current customers, partners, and suppliers of GIAC Enterprises can authenticate into the site and view and access information only pertinent to them.
- Access to the protected and secured areas requires various layers of authentication. The primary firewall (with an additional secondary firewall to serve as a failover firewall) and additional nested firewalls have been placed to provide multiple layers of defense. Within each subnet, an intrusion detected tool monitors for suspicious and malicious traffic to and/or from servers.
- In addition, copies of all server logs are maintained in a dedicated Syslog server.
- All employees have been required to attend an orientation workshop during the first week of employment that covers GIAC's rules and policies regarding information security topics.

This security assessment has brought forward several **opportunities for improvement:**

- Strong password policies must be established, documented and enforced. The password length must be system enforced to be 6 to 14 characters long and password expiration should be automatically enforced as well. In addition, a password cracking program should be run periodically to detect any accounts with passwords that can be easily cracked, and a warning mail is sent to these accounts and passwords are expired. GIAC internal users and GIAC partners and suppliers should be educated that passwords should contain at least two numbers and two letters, and upper and lower case letters should be mixed. Any word that is in a dictionary, or any names, places or personal information such as birth dates should not be chosen.

- Security reports produced by the intrusion detection tool must be regularly reviewed by the Information Security Officer and any incidents requiring further explanation should be investigated. Such logs are helpful for intrusion and fault detection analysis.
- The Information Security Officer should regularly carry-out additional corrective actions as deemed necessary (i.e., server hardening, applying new patches, security policy development/modification, and firewall

configuration).

- Updated policies and procedures should be made available and communicated via the company Intranet.
- GIAC's senior IT management and supporting staff should periodically attend security training and certification programs to keep abreast about the latest and best industry practices.

Risk 2: Virus or other malicious software attack to the GIAC Enterprises network.

- **Description of the Risk**

Viruses, worms, and other malicious software attacks represent a major concern for computer and network security. A virus is designed to cause damage to an application or network component. A virus usually resides within another program or document. Once the program is run or the document is opened, the virus is executed. Another popular malicious program is a worm. A worm resides in active memory and replicates and duplicates over computer networks. Unlike a virus, it does not attach itself to a host program, but rather tricks the receiving network program into installing and executing their own copies of the worm.

Software attacks also pose a strong threat to networks. For example, one of the greatest threats come from such sophisticated attack software as a Trojan Horse. Basically, a Trojan Horse resides within what appears to the user to be a normal and useful software application. When the user unintentionally activates the Trojan Horse, the program begins to perform actions the user never knows about or intends. GIAC Enterprises realizes that conventional anti-virus scanners will detect and remove many known malware programs that are distributed; however, GIAC's ITD department must add certain behavioral and procedural changes in order to catch viruses and worms.

- **Justification for Company Concern of This Risk**

GIAC Enterprises business operations would be considerably disrupted or even halted as a result of a virus or other malicious software attack. A virus could infect a critical database server or even result in complete loss of information. For example, if a virus were to infect any of GIAC Enterprises' servers, major business disruption, alteration, and loss of data could occur. GIAC Enterprises' first and foremost concern is the patient data that it must house on its servers in order to process the insurance claims.

The loss of patient information is possible if a malicious virus, worm, or other malicious software were to infect the application systems and the respective servers and databases. In addition, an attack in the form of a virus or other malware program could compromise the integrity of data and either halt operations or supply incorrect data for daily automated operations (i.e., information posted to the website; information that partners, suppliers, and customers access; claims filed to the insurance companies, etc.).

A malicious software program can disguise itself within our company's applications and systems and result in the transmission of critical business data to unauthorized recipients or it could cause an unwanted financial transaction to be processed. For example, Trojan Horse programs, such as the commonly known BackOrifice, SubSeven and Netbus, could be set to allow unlimited access to GIAC company databases and servers bypassing security monitoring. With access to GIAC computers, a hacker can run any program or download our database, servers, and application passwords and files.

With the high threat of such viruses and malicious software a prevalent risk, GIAC Enterprises understands that any vulnerability on our part either through lack of anti-virus tools, access to virus updates, or untrained IT personnel will result in an exploitation of this risk. Although GIAC Enterprises has the technology in place to mitigate the risk of viruses, certain behavioral changes as well as documented and enforced policies must be established.

- **Possible Consequences from an Exploitation of This Risk**

Successful execution of viruses or other malicious software within the company's network would result in such consequences as loss of customer trust, tarnished image with business partners, and ultimate legal action against the company. A virus could infect file and database servers leading to the destruction of critical data. GIAC Enterprises' business productivity would be greatly affected until the data recovery process is completed.

If a worm program were to enter the GIAC network, it could occupy much network bandwidth as it continued to replicate across the network causing system degradation. In addition to possibly destroying the integrity of our data, the worm could potentially cause an overall shutdown of GIAC operations and communications since users cannot access IT resources due to low or nonexistent bandwidth. Overall, the reputation and brand image of the company would be greatly compromised, perhaps resulting in heavy and unrecoverable financial losses and legal action.

Furthermore, through the use of a Trojan Horse program a hacker could falsely portray GIAC Enterprises' company computers as the originator for the hacker's attack on other companies. Attacks that trace back to our company would result in legal action taken against us, and false negative publicity to our customers, partners, and suppliers. Also, our own computers can be used in Denial Of Service (DoS) attacks against us, where many machines simultaneously request

information from a particular GIAC Enterprises server, flooding it with requests until it crashes. Ultimately, GIAC Enterprises' business operations would come to a halt, and such repetitive events would damage our reputation resulting in financial losses and possible legal action.

- **Risk Mitigating Steps**

Several risk mitigating steps have been laid out to reduce the possibility of a virus or other malicious software to enter the network. Anti-virus software and tools have been installed on the following network and client components:

- Company Desktops and Remote User Laptops: All GIAC Enterprises desktops and remote user laptops are installed with the latest anti-virus software. Anti-virus updates are pushed out to the user community.
- E-Mail Relay Gateway Server and Internal Mail Server: Both the GIAC Enterprises E-Mail relay gateway server and internal mail server have anti-virus software installed on them.
- File and Database Servers: All file and database servers have been installed with the anti-virus software. The latest definition file updates are applied to the servers immediately to ensure consistent protection.
- Firewalls and Intrusion Detection Tools: Several layers of firewalls are prevalent throughout the network. In addition, a dedicated intrusion detection tool for each subnet monitors its own segment to prevent the launch of trojan programs, viruses, and other malicious software within the network.
- In addition, regular system backups are performed, both to a mirrored hard drive and to tape media. Also, backup tapes are sent offsite for storage.

However, this security assessment has brought forward several **opportunities for improvement:**

- The GIAC Enterprises' user community should be trained on the proper procedures that they should follow to prevent or take action to eradicate a computer virus and other malicious software.
- An improved, documented, and enforced Anti-Virus Policy should be established, and, on a regular basis, communicated and made accessible to the user community.
- The GIAC Information Technology Department (ITD) should establish a policy on the employee use of GIAC Enterprises' IT resources.
- The ITD department should install a URL filtering and blocking software that can automatically deny GIAC users entry into sites that involve:
  - **Web-based E-mail**: Since web-based E-mail programs can

circumvent GIAC's mail server and ultimately our company's virus scanning systems.

- **Adult Content**
- **Entertainment** (mp3 downloads, etc.)
- **Hacking**
- **Gambling**, and any additional categories as GIAC Enterprises senior management sees fit in the best interest of the company's security.

Risk 3: Unauthorized System and/or Database Changes.

- **Description of the Risk**

GIAC's information systems are among its most valuable assets that connect it with its customers, partners, and suppliers. Significant expenditure of time and resources are spent in maintaining or integrating existing applications, databases, networks, and platforms. However, this security risk assessment has identified the need for an efficient change management process to be incorporated in business practices to appropriately handle requests and prevent unauthorized system and/or database changes.

Currently, in the IT system development environment appropriate segregation of duties has been applied. However, there is no formal established, documented, and enforced change management process in place. Until now, an unauthorized or accidental change made by GIAC developers has had minimal impact on operations. However, as GIAC Enterprises continues to grow its customer base and number of internal employees, there is a high risk of an unauthorized change occurring. GIAC Enterprises realized that unauthorized system changes by GIAC's developers and other IT personnel can result in serious damage to the processing of medical claims or customer, supplier, and partner information. In addition, other data such as company proprietary information and financial transactions could be compromised.

- **Justification for Company Concern of This Risk**

GIAC Enterprises business operations and information processing functions occur on company information systems interacting with internal critical databases. An unauthorized change brought into the production environment of live systems and databases could interrupt or even halt business operations. GIAC Enterprises feels that a lack of a detailed change management process is a large vulnerability that weakens GIAC Enterprises ability to mitigate the risk of unauthorized system and/or database changes.

Certain current processes in the GIAC development environment could easily cause a manifestation of this risk. For example, requests that are placed by a user via the telephone, e-mail, or face-to-face conversations are not currently logged or captured in any central repository. A developer who receives the phone call may make the change without any written record of the originator of the request and the reason for the change. In addition, any analysis or research performed in order to implement the change is not captured in any documentation. Such formal documentation would facilitate team communication between the developers, analysts, and management. Since there is no formal change management process, available staff resources are assigned change requests on an ad hoc basis, and final changes that are made and moved from the test environment into the production environment do not receive official sign-off by the user and project managers. Such undocumented changes do not provide any audit trail or proof of the necessity for the change. If the GIAC Enterprises' systems and databases continue to undergo changes with no formal change management process, it will result in serious operations, reputation, and legal problems for the company.

- **Possible Consequences from an Exploitation of This Risk**

Unauthorized system changes can result in inaccurate behavior of GIAC programs and systems. In turn, this will result in negative consequences for the company. Some consequences include the inability to react quickly to business initiatives or recover from system problems and adverse impacts on revenue, business partnerships, or value-adding elements of IT infrastructure due to system dysfunctions or unavailability. In addition, a loss of highly skilled personnel due to ineffective workload management and a loss of competitive market position and public image can occur.

During this security risk assessment, meetings with GIAC Enterprises' IT personnel have revealed that the ITD department experiences reduced productivity and efficiency especially between developers/programmers, project managers, and management due to a lack of a defined change management process. For example, developers' and analysts' responsibilities and ownership for requests are often unclear. In addition, notification of successful changes is not communicated in a consistent manner. Often other team members of the development team are unaware that a change has been made and closed out. The lack of communication and documentation often leads to a duplication of efforts.

Next, GIAC Enterprises recognizes that unauthorized system/database changes can produce a negative effect on the company's reputation and business revenue. For example, if a developer applies an unauthorized change to the claims processing system on the production server, this could compromise the functionality of our company's ability to process the insurance claims. Such events would tarnish our reputation with customers and decrease the likelihood that they

would select GIAC Enterprises over our other competitors. In addition, a lack of a change management process would harm opportunities for positive findings of IT security audits that may be performed. Furthermore, a lack of a documented change management process for each request would increase GIAC Enterprises' risk for legal action if any unauthorized change manages to process customer's claims incorrectly or without adherence to such regulations as the Office of Inspector General (OIG) Third Party Billing Guidelines and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- **Risk Mitigating Steps**

GIAC Enterprises understands the importance of a controlled and effective change management process. Currently, **various processes carried out** that contribute to minimizing the risk of unauthorized system changes and maximize effective recovery in the event that an unauthorized change does occur include:

  - Regular system backups are performed, both to a mirrored hard drive and to tape media. In addition, backup tapes are sent offsite for storage.
  - Only authorized personnel have access to the platform, network, and database layers of each environment.
  - Production system outages are well-planned and communicated to users.

However, in order to best mitigate the risk of unauthorized changes to the production environment, the following **opportunities for improvement** should be followed:

  - Strong password policies must be established, documented and enforced. The password length must be system enforced to be 6 to 14 characters long and password expiration should be automatically enforced as well. In addition, a password cracking program should be run periodically to detect any accounts with passwords that can be easily cracked, and a warning mail is sent to these accounts and passwords are expired. GIAC internal users and GIAC partners and suppliers should be educated that passwords should contain at least two numbers and two letters, and upper and lower case letters should be mixed. Any word that is in a dictionary, or any names, places or personal information such as birth dates should not be chosen.
  - An IT systems and database change management policy should be developed and communicated throughout the Information Technology Department. In addition, the general user community should also be made aware and have access to the documented change management process so that they understand the process of any request they may place to ITD.
  - Change requests should be prioritized and resourced by business and IT

management. The design of major requests begins with prototypes, while the requirements of minor request enhancements and fixes are defined for development.

- The request coordinator should capture requests, forward them for analysis, and handle the request management process to track and communicate request statuses for users, and to escalate high priority and outstanding issues. Business and technology analysis should be performed on the request to determine business impact and justification, feasibility, and initial resource needs.
- The organization should strive for continuous improvement to the change management process, frequently updating policies, procedures, and performance metrics as needed.

Assignment 3: Evaluate and Develop Security Policy

GIAC Enterprises Current Anti-Virus Policy

Please Note: The following policy is based upon an existing policy in use at this practical assignment's author's company. The author of this paper feels that his own organization is still at an initial stage in its security policy and procedures documentation development, and welcomes such an opportunity to critique his organization's current anti-virus policy. The author looks forward to improving documented policy as an Information Security Officer at his organization.

GIAC Enterprises has a documented Anti-Virus Policy. The current policy is attached below.

GIAC Enterprises Information Security Policies

Anti-Virus Policy

Last Revised: 11/05/2002

FOR INTERNAL USE ONLY

Purpose:

This document provides GIAC Enterprises policy on anti-virus software.

Policy:

The ITD requires that all computers, servers, and remote user desktops/laptops have the appropriate anti-virus software installed on them.

Responsibility:

The ITD will be responsible for installing the anti-virus software and communicating the importance of its use to the GIAC user community. In addition to the installation of anti-virus software, the ITD will respond to user inquiries and user virus reports and perform regular virus scans of the server system files and staff server file store. Also, each department within the company and individual users must adhere to this policy statement.

Critique of Original Policy and Revised Anti-Virus Policy

The current anti-virus policy for GIAC Enterprises is a very general policy. Although it provides the company with a starting point in terms of a documented policy, it does not elaborate on key aspects that a sound and comprehensive policy statement should.

Policy Positives (+)	Policy Areas for Improvement
• The policy provides the organization with a documented policy.	• Although the **purpose** of the policy is stated, the policy is not detailed enough. The policy does not include any information on how high of a risk virus and malicious software pose to the health of the company or why the policy is established.
• The policy on anti-virus software is clearly stated to describe that the anti-virus software is required on all computers, servers, and remote user desktops/laptops.	• Although the policy does not contain a **background** section, its existence would further strengthen the user's understanding of the need and justification for the anti-virus policy.
• The policy lists the basic responsibilities that the Information	• Within the context of its purpose statement, the current policy lists the

Policy Positives (+)	Policy Areas for Improvement
Technology Department assumes to ensure that anti-virus protection in place in the company.	extent of the anti-virus policy (i.e., all computers, servers, and remote users' desktops/laptops). However, it is a more clearly organized policy if what computers are covered by this policy is listed under a separate **scope** section.
	• Although the policy lists the general **responsibilities** of the ITD, it would be beneficial if additional detailed responsibilities were to be included. • In addition, the anti-virus policy should also outline who can modify the existing policy. • Since the success of an effectively implemented anti-virus policy also relies on the active commitment and support of both the various departments within GIAC Enterprises and each user, their responsibilities should also be included.
	• This policy lacks an **action** section. The addition of an action section is necessary to detail what specific actions will need to occur for certain situations. • In addition, a disclaimer should be included describing what will occur if the individual(s) responsible for launching the virus or malicious software attack against the company are found guilty.

GIAC Enterprises Revised Anti-Virus Policy

GIAC Enterprises Information Security Policies

Anti-Virus Policy

Last Revised: 12/20/2002

FOR INTERNAL USE ONLY

Table of Contents

1.0 **Purpose**
2.0 **Background**
3.0 **Scope**
4.0 **Policy Statement**
5.0 **Responsibility**
6.0 **Action**

1.0 Purpose

The purpose of this policy is to identify and detail the anti-virus measures established by the Information Technology Department (ITD) of GIAC Enterprises to prevent infection of computers and computer systems by computer viruses and other malicious software. Due to the nature of GIAC's business operations with the Internet, there is a high risk of an attack to the network via a virus or malicious software. This policy is intended to prevent major and widespread damage to the network's applications, files, and hardware.

2.0 Background

A major key to the continued success of GIAC Enterprises as a leader in the medical billing industry is its commitment to ensuring security of its information systems. In addition, as a service provider to the healthcare industry, GIAC Enterprises must ensure that it is compliant with patient confidentiality as mandated by the Office of Inspector General (OIG) Third Party Billing Guidelines and HIPAA regulations.

3.0 Scope

This policy is applicable to all GIAC Enterprises user desktop computers, servers, and remote user desktops/laptops.

4.0 Policy Statement

- Standard and supported anti-virus software will be identified by the ITD.
- All computers and servers on the company network must have the ITD standard and supported anti-virus software installed on them.
- All remote access user laptops must have the appropriate anti-virus software installed on them prior to issuance of remote VPN access.
- Both the public E-mail relay server and the internal mail server will have anti-virus software installed on them.
- All file and database servers will have the appropriate anti-virus software installed on them.
- Updated virus signature file or antivirus configuration changes are pushed out to the servers, user desktops, and remote users' desktops/laptops and anti-virus scans will be scheduled to run at regular intervals.

5.0 Responsibility

Information Technology Department (ITD) Responsibilities

- Maintain and modify this anti-virus policy in accordance with the document change management process established by the ITD department.
- Arrange for sufficient anti-virus software licenses for GIAC Enterprises workstations and servers.
- Educate and communicate to the GIAC user community on a regular basis about the importance of anti-virus software, how the anti-virus software virus file updates will be done, and make this company policy easily accessible for viewing.
- Maintain up-to-date anti-virus products.
- Respond to user inquiries and user virus reports in a timely and professional manner.
- Take appropriate action to contain the virus and/or malicious software infections and assist in their removal.
- Maintain ITD staff knowledge and expertise on viruses and virus protection through training and access to resources.
- Perform regular scans of server system files and staff server file store.

Departmental Responsibilities

- Any department that manages its own servers must use the ITD standard and supported anti-virus software.
- Any new workstations or laptops purchased by an individual department must be identified to the ITD to ensure proper anti-virus software is installed.

Individual User Responsibilities

- Take preventive measures (i.e., ensuring anti-virus software is not disabled or uninstalled) to protect against virus infection and failure to do so may constitute an infringement of GIAC Enterprises regulation regarding the use of company resources.
- Contact the ITD for assistance immediately if a workstation or laptop is suspected to be infected.

6.0 Action

Appropriate action will be taken by the ITD based on the nature and extent of the virus/malicious software detected. In addition, any individual(s) found to have caused the virus/malicious software attack against the company or to have violated this policy may be subject to disciplinary action, up to and including termination of employment and legal action.

Virus/Malicious Software Attack on a Single or Isolated Cluster of Computers

- If a virus or malicious software is detected on a computer, the IT Helpdesk must be contacted immediately.
- An IT technician will remove the virus/malicious software either by visiting the work site or via screen-sharing software.
- If the technician is unable to remove the virus/malicious software, the infected computer(s) will be removed from the network, have its hard drive reformatted, and all software reinstalled with clean, licensed copies.
- Once the computer(s) are verified as being virus-free and/or malicious software-free by the ITD, it will be reconnected to the network.

Widespread Virus/Malicious Software Attack on the Entire Network

- In the event that a widespread virus and/or malicious software attack is spreading across the network or has great potential to cause such widespread damage, the ITD will separate GIAC Enterprises from the Internet by either fully or partially removing a service, such as E-mail and may disconnect all workstations from internal network privileges.

The temporarily partial or full services that were disconnected will be restored once the ITD determines that no threat remains to the company's network and resources.

Assignment 4: Anti-Virus Software Installation Procedures

GIAC Enterprises Information Security Procedures

Anti-Virus Software Installation for Windows 2000 Workstations

Last Revised: 12/20/2002

FOR INTERNAL USE ONLY

Purpose

The purpose of this procedural document is to define how the anti-virus software installation component of implementing the GIAC Enterprises Anti-Virus Policy should be handled.

Significance/Importance of Procedure

Implementing information technology security measures within GIAC Enterprises is critical to our success. Since our business operations thrive on the use of technology, and we regularly interact and communicate with our customers, partners, and suppliers via the Internet, we are susceptible to serious virus and other malware program infections. This anti-virus software installation procedure for the Windows 2000 workstations in use at our company is an integral part of implementing a strong defense mechanism for our network against virus and malware program attacks.

Responsibilities

The Information Technology Department (ITD) is responsible for the installation and configuration of the anti-virus software on Windows 2000 workstations.

Actions

Step-by-Step Installation of McAfee VirusScan on Windows 2000 Workstations

1. To begin the installation, click on **vscan.exe**. You will then see the Setup welcome panel. This panel will tell you the location of the README.TXT file.
2. Click the **Next** button. The next panel displays the end-user license agreement, which you should read carefully.

3. Next, you will select the security mode you wish to use, Maximum or Standard. Choose **Use Maximum Security**. By selecting this option, users will be required to have Administrator rights to the workstation in order to make modifications to any configuration settings.
4. After clicking **Next**, you will be asked to choose the type of installation, whether Typical or Custom. Choose **Typical Installation**.
5. After clicking **Next** again, select the **Install** button. After removing any incompatible software, the VirusScan program files will be copied to the workstation hard disk.
6. Next, select the checkbox labeled **Scan Memory for Viruses before Configuring**. When you click on the **Configure** button, the VirusScan application will scan the system memory for viruses before it continues. If an infection is found, you will be alerted and given a chance to respond to the virus.
7. The next option is to **Run Default Scan for Viruses after Installation**. This checkbox is selected by default. **Clear this checkbox** and skip to the next menu.
8. You will then be given a choice of three configuration options, **Run AutoUpdate Now**, **Configure AutoUpdate Now**, and **Wait and Run AutoUpdate Later**. Select **Run AutoUpdate Now** so that the utility will connect directly to the McAfee website and download the latest .DAT file updates. By choosing this option, you will be sure you are scanning using current files. Click on the **Next** button for this process to begin.
9. Finally, select the **Start VirusScan** checkbox and click on the **Finish** button. The VShield scanner and VirusScan Console icons will appear in the Windows system tray. Your application is now installed and ready to be used.

Verification of Workstation Anti-Virus Software Installation and Ensuring Consistent Compliance to Meet GIAC Enterprises' Anti-Virus Policy

Verification of the appropriate anti-virus software installation on GIAC Enterprises will be managed by the ITD. There are two categories of workstations that need to be accounted for: new workstation purchases and existing workstations in the network.

<u>New Workstations</u>:

Any new technology acquisitions, whether for ITD or other departments within GIAC Enterprises, must be made through the ITD. Therefore, any workstations that are purchased will be configured with the standard desktop applications per ITD standards.

- One of the standard applications to be installed is the anti-virus software.
- Before a workstation is issued to a user and connected to the live GIAC Enterprises' network, the ITD will sign-off in the central technology asset log that,

among other key office suite software and operating system software, the approved anti-virus software has been installed.
- Once the workstation is issued to the user, he/she must sign-off that he/she has received and understood the GIAC Enterprises Security Policy Guide (in which the GIAC Anti-Virus Policy is included).

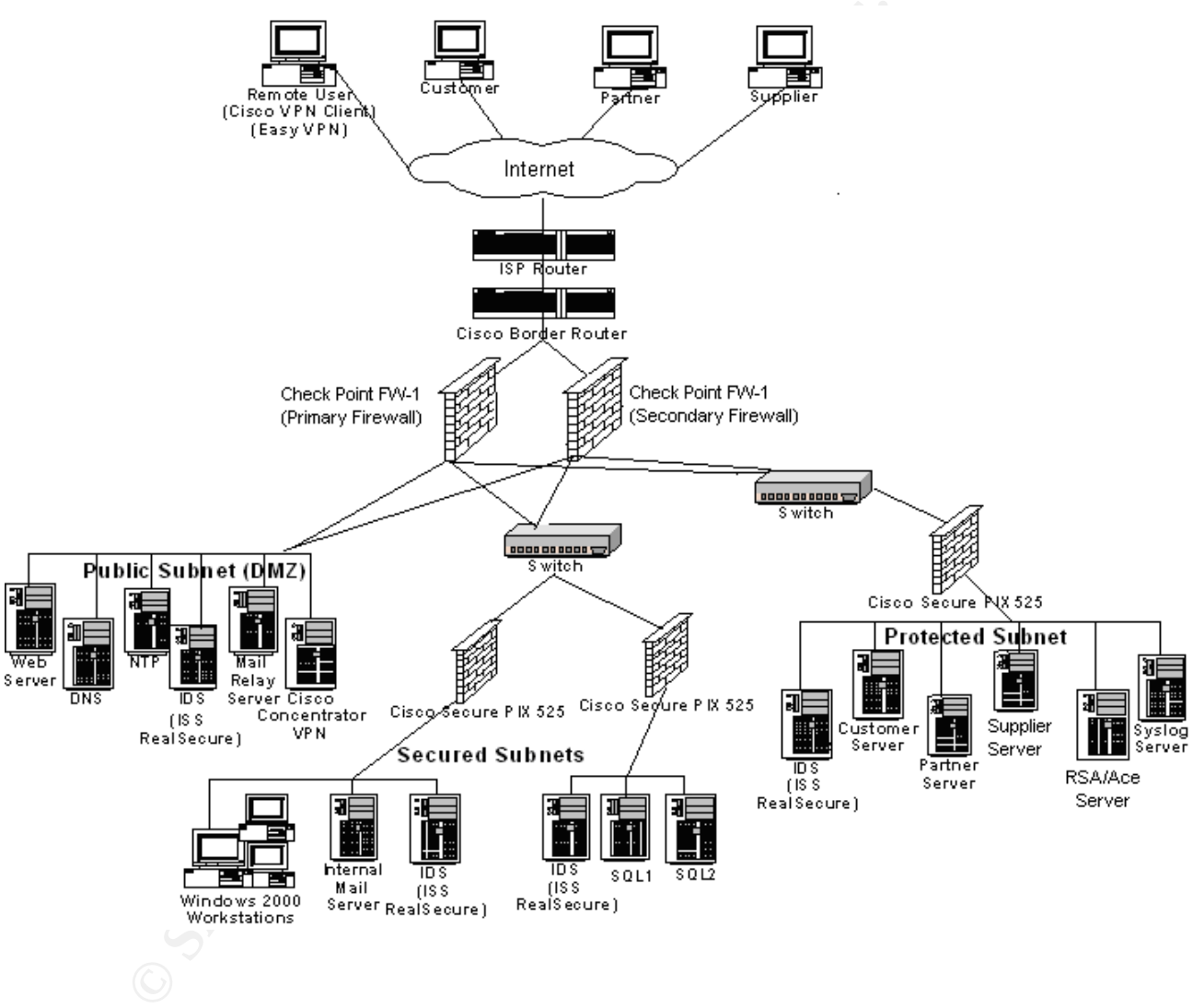
Existing Workstations Connected to the Network:

The GIAC Enterprises user community is to be notified on a periodic basis of the fundamental security measures and goals that the organization needs to meet. Included in those measures is the anti-virus policy, in which it states that users should not uninstall or disable the workstation's anti-virus software. Furthermore, the ITD will notify the user community of any anti-virus software updates to newer versions or change in approved software and conduct the appropriate installation procedures.

In addition, in order to measure and ensure employee compliance with the need to have active anti-virus software running, security audits should be performed by third party firms, once every six months. Any departments lacking compliance with the anti-virus software policy must be reported to the Senior IT Management and appropriate follow-up actions must be taken to ensure compliance.

Appendix I: Network Diagram

Key concepts for the development of GIAC Enterprises' network layout were gathered from external sources (Cisco Systems 18-20; Zimmerman 5).



References

Cisco Systems. “Chapter 1 Understanding the Network Topology.” Cisco Secure Policy Manager Administrator’s Guide: Network Topology Definition. 4 Jun. 2000 URL: http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver21/topology/nwunder.pdf (2 Dec. 2002).

CyberGuard Corporation. “Auditing and Intrusion Detection, A CyberGuard Corporation White Paper.” April 2000 URL: http://www.bluesky.com.au/Products/CyberGuard/WhitePapers/auditing.pdf (15 Oct. 2002).

Krychiw, Steven. “Secure ID: A Secure Two Factor Authentication.” SANS Institute. 28 Feb. 2001 URL: http://rr.sans.org/authentic/securid.php (15 Sep. 2002).

United States of America. National Security Agency. “Defense in Depth.” National Security Agency Recommendation Guides. URL: http://nsa2.www.conxion.com/support/guides/sd-1.pdf (12 Dec 2002).

VeriSign, Inc. “What is the difference between a VeriSign 40-bit SSL certificate and a VeriSign 129-bit Global Server ID?” URL: http://www.verisign.com/products/site/faq/40-bit.html#basics3 (24 Oct 2002).

Zimmerman, Scott C. “Secure Infrastructure Design.” Internet Security Alliance. 1 July 2002 URL: http://www.isalliance.org/resources/papers/Secure_Infrastructure_Design.pdf (5 Nov. 2002).