Global Information Assurance Certification Paper

THE GIAC ENTERPRISES

Information Security Officer Certification Practical
(GISO VERSION 1.2)

By

Charles Iheagwara, Ph.D., PE

SANS INSTITUTE
June 25, 2002

Table of Contents

1.0 ASSIGNMENT 1 – DESCRIBE GIAC ENTERPRISES

1.1 DESCRIPTION OF GIAC ENTERPRISES

The GIAC ENTERPRISE provides financial news and information service derived from U.S. Securities and Exchange Commission data to stock market watchers and the general public. This is provided as a service for GIAC's customer, the NARRASSSDAAYQ stock exchange market. Based in Newark, Connecticut, with offices in Roseville and Baltimore, Maryland, and New York City, New York the company sells to the corporate market and Internet portals as well as running destination Web sites including GIAC ***Online*** (http://www.GIAC-online.com).

The company is also a developer of financial and business system solutions and specializes in providing and hosting E-commerce application development and management services to clients using different Web and database technologies.

The GIAC ENTERPRISE is well known in the industry for providing exceptional customer services. The company does business across the world, but between 75-85% of its clientele is based in North America. The company currently employs a little over 2300 employees.

1.2 DESCRIPTION OF IT INFRASTRUCTURE

1.2.1 Overview

The GIAC enterprise IT infrastructure is a system, which interconnects a multitude of computers and workstations for the purpose of communications and information/resource sharing. To keep the various interconnected parts of the system interoperable, appropriate data transport and exchange technologies, rules and procedures are implemented.

The GIAC ENTERPRISE network design incorporates an outside network, a DMZ network and an internal network. Among the mission-critical servers/devices in the network system are VPN, Web, FTP, DNS/Mail servers, routers and PIX firewalls with redundant failover mechanism and a Cisco local director for load balancing.

The topology of the network (Figure 1) features the following:

- A front end outside network (10.33.242.0) with desktop support (Help Desk) server,
- A DMZ intermediate network (10.178.213.0) with Web, FTP, DNS/MAIL servers etc.;
- A back end internal network (10.172.162.0) with workstations and support servers linked through a firewall to the DMZ and front-end outside network.

The IT infrastructure consists of two perimeter routers on two alternate Internet routes. The two serve as redundant routes to ensure unimpeded Internet access. There are also two firewalls with hot standby redundant configuration.

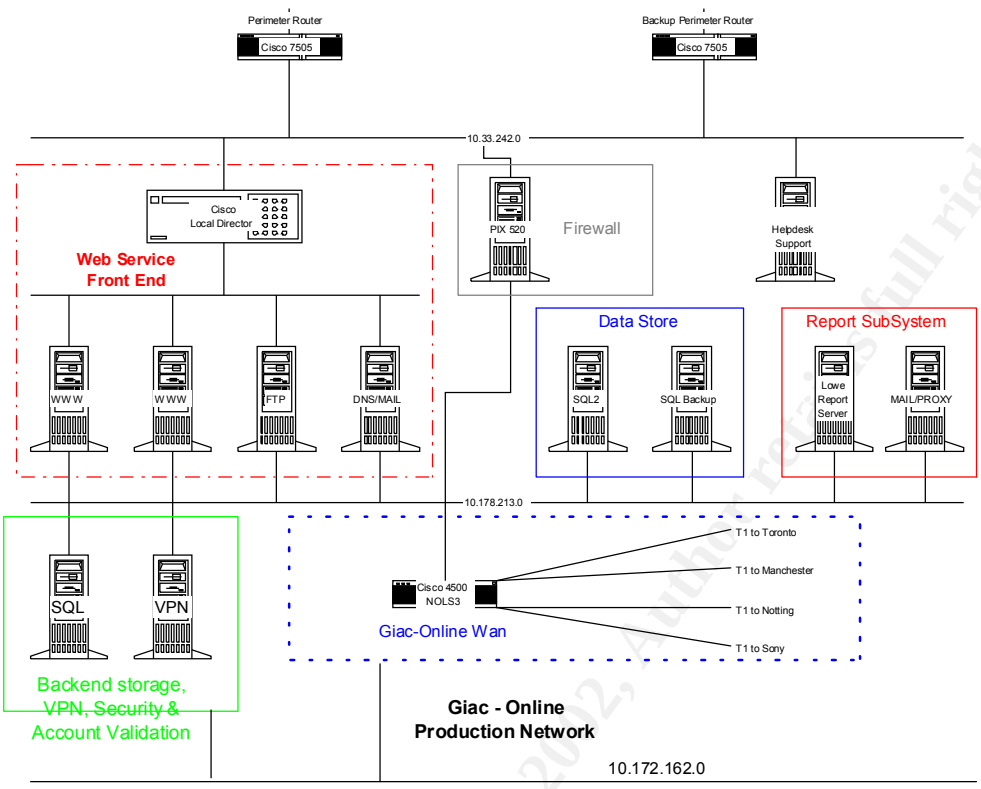

Figure 1 The GIAC ENTERPRISES network

The centerpiece of this design is using firewall to centralize access control to the internal network. A firewall [1] is a safeguard that one can use to control access between a trusted network and a less trusted one. The main function of a firewall is to centralize access control. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted.

The network is of distributed architectural topology. The outside network incorporates a help desk support server used to render customer support services. The DMZ system consists of a collection of trusted single hosts, networks and multilevel file servers. Business service servers (Web, FTP, DNS, etc.) are the major component of the system. The DMZ network is the intermediary network that sits between the front-end outside network and the actual hosts/servers on the protected internal network.

The GIAC's design's standard for all networking components is Cisco. Based on this, the initial level of fault tolerance includes two PIX Firewalls as the entry point to the Internet and to the corporate network. Using the "PIX Firewall fail over option" the design eliminated a single point of failure for the Internet and the corporate backend (internal protected network). Basically, with two PIX Firewalls running in parallel, if one malfunctions, the second PIX Firewall transparently picks up and keeps things running. One thing to remember is that the second firewall is a standby hot failover and does not

provide any level of load balancing. Hence there is a Cisco load balancing local director for the Web servers. Dial-in Remote Access Service is also incorporated into the design.

The major network servers and devices are described below.

1.2.2 Web Servers Configuration

The Web servers are Intel-based Pentium 500mhz systems with dual processors and 256MB RAM. They are configured with Windows 2000 advanced server (Service Pack 2) operating system and form a cluster farm with load balancing. The super fast caching scheme is implemented on the Web servers.

1.2.3 Websites description

The Web sites are the corporate sites of a major stock exchange market hosting multimedia applications that include video graphics, database applications, and financial news contents. Each site can handle up to 10000 concurrent connections.

1.2.4. Desktops

GIAC uses Intel based desktops and laptops, which run Windows NT 4.0 (SP6a) or Windows 2000 (SP2). Currently, over 1543 workstation nodes are supported. This number includes those used by remote logins

1.2.5 Databases Systems

SQL, Oracle, Informix and Access database systems are used throughout the company. The SQL databases host the financial market data as well as shareholder data. The trading system uses an Oracle database. The accounting system is powered by an Informix database and our CRM is built on a SQL platform. Access is used for "user" database functions and reporting.

.

1.2.6 Servers

There are SUN Solaris servers running Solaris 2.8. There are also running Intel based Windows servers, running either Windows NT (SP6a) or Windows 2000 (SP2). The Windows environment primarily houses the production/customer data, while the Solaris servers are used for a few application, file and print services.

1.2.7 Network

GIAC is Cisco-centric. Layer 2 switching is achieved by using Cisco 4500's at the closets and layer 3, using Cisco 7505's, at the core. Each closet has diversely routed fiber connecting it back to the core. Each desktop is given a 10/100 Ethernet port and servers are either 100 or 1000MB full duplex copper connected Ethernet.

GIAC's remote offices (Toronto, Manchester, Notting, Sony) are connected via private T1 line with no Internet outlet. Internet access is routed to GIAC's outlet through the PIX firewall and perimeter router. Offices needing voice connectivity are connected via T1, with some portion of that circuit dedicated to voice. Employees of the firm who require access to company data while out of the office use the VPN over the Internet. The VPN employs Cisco's VPN hardware - VPN3000 series concentrator.

1.2.8 Firewalls / Load Balancers

The GIAC ENTERPRISE uses Cisco's PIX 520 Firewalls and Cisco's local director for load balancing across the Web servers.

Device	Vendor	Usage	Connectivity
Pix Firewall 520	Cisco	Authentication of network access for applications	Ethernet Interface 100Mbps
Router	Cisco 7505	Authentication based on access list (filtration)	Internal: 100Mbps Ethernet Interface to Pix firewall. External: T1 connection to the Internet.
Proxy Server	Microsoft	Authentication based on applications	Ethernet Interface 100Mbps for internal and external connections
Switch	Cisco 4500	Routing and Switching	Ethernet Interface 100 Mbps

Table1: Features of the IT network security routing equipment

1.3 BUSINESS OPERATIONS

GIAC Enterprises' business involves the transmittal of financial news information and data generated from the SEC fillings of companies to market watchers worldwide over the Internet. This is provided as a service to the individual companies that trade on the NARRASSSDAAYQ trading index stock market. Thus, the company is primarily a direct marketing firm, which utilizes direct marketing techniques to disseminate the stock market values of the different companies to the general public. In this case, the stock market (NARRASSSDAAYQ trading index) is GIAC's customer. The marketing techniques typically direct customers and the general public to the transactional Internet portal (GIAC stock market Web site) and offer access to a toll free customer contact center for customer service support. Approximately 85% of the GIAC's business is done over the Internet.

Financial News Dissemination Process: In the GIAC ENTERPRISE network setup, Front End Web server financial news data streams are fed from backend SQL servers. The SQL servers receive their data input streams from a global cache to the LAN system (Figure 2).

Fundamental information and the most recent values of real time information received from Bridge Ticker Plant are transmitted to the Global cache database. The Ticker data in the Global Cache is then sent over to the SQL server in the network (LAN/WAN) using either a UDP broadcast or TCP connection. In this way transmittal of financial data is realized. The global cache provides LAN users with access to Bridge's global ticker data.

Bridges global ticker contains real-time and fundamental information on over 500,000 securities from over 130 exchanges and more than 400 market makers.

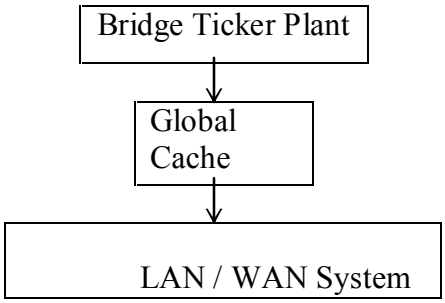

Figure 2 - The Ticker Bridge traffic flow

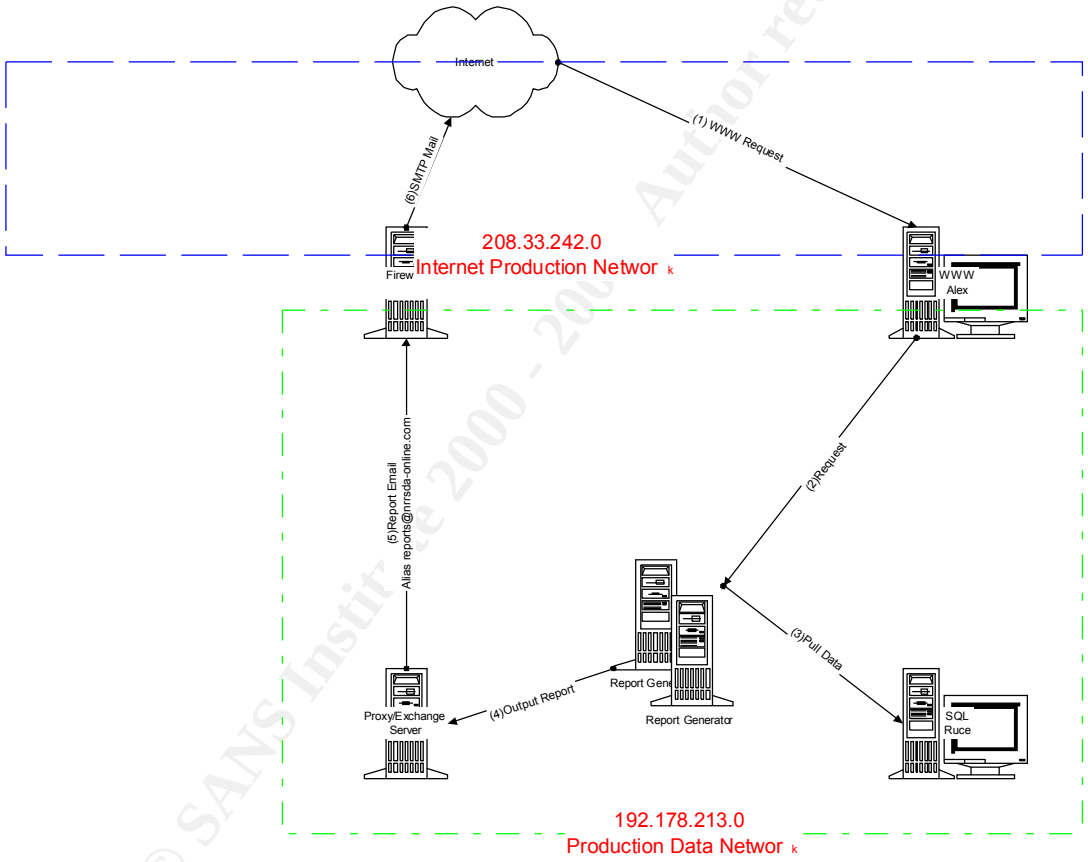

Figure 3 – Traffic flow pattern

Figure 3 is a representation of the traffic flow pattern from the production of financial news through its release on the Internet. Any one can easily log on to the GIAC Web site at: (http://www.GIAC-online.com) to get the latest stock market price for member companies of the NARRASSSDAAYQ trading index.

Web Site: The GIAC Web site is very busy with more than 10,000.00 concurrent connections. Due to the high volume of transactions and the varied nature of the transactions, the Web site is designed to ensure high Internet availability with privacy safeguards. In this regard, GIAC's systems and staff are available to all (business associates, the general public and customers) 24 hours a day, 7 days a week, 365 days a year.

Thus, the requirements [2] for performance, reliability, speed and operational support of the e-business activities of the corporate GIAC ENTERPRISE systems are complex and extremely high. In terms of reliability, the system is designed to ensure system-level availability of 99.999% on a 24x7 basis. In terms of operational support, the system must meet all of the requirements to be certified for operation. These requirements also incorporate security schemes into the product(s) design as a precursor to meeting all functional requirements established for the system. The implementation of the security scheme should be able to support these requirements in a manner that does not impede vital system performance indexes such as desirable low values for end-end-latency, Web request-response time, network throughput and protection of the privacy of data.

Because of the nature of GIAC's business transactions, uninterrupted Internet access is guaranteed by incorporating a redundant backup Internet route. Telecommuters/Remote users can also access network resources through a backend VPN server.

Remote Access Requirements: In order to successfully conduct business with GIAC Enterprises, customers and business associates need to have consistently reliable telephone, fax, email, Internet, file, print and data base access, whether in a remote office or in our main campus facilities. GIAC sales associates must also have the same system reliability and availability while remotely accessing the corporate systems over our VPN (Virtual Private Network). These remote users are primarily sales associates who connect to the VPN over some sort of broadband technology. The remaining associates need VPN access while traveling, which is typically dial-up access.

Regulatory requirements impact on the way GIAC transacts business. GIAC is a member of a highly regulated industry. Transactions of financial service organizations are governed by the SEC (Security and Exchange Commission) regulations as well as other regulatory agencies such as the NASD (National Association of Securities Dealers). As of July 1, 2001 we are also legally obligated to safeguard our customer's confidential information we are transmitting between our customers, vendors and even amongst ourselves. This legal obligation is imposed under the Gramm-Leach-Bliley Act and Regulation SP.

Hosting Service: GIAC is also a Web Site host service provider for institutional businesses that market financial service products to their customers on the Internet. Activities associated with this typically account for about 15% of GIAC's business.

2.0 ASSIGNMENT #2 - AREAS OF RISKS

2.1. BACKGROUND INFORMATION ON RISKS AND MITIGATION MEASURES

2.1.1 Risks: The enterprise network usually offers several possibilities for data to leave or enter a specific computer. Computers can have individual modems with a variety of available connection scenarios e.g. RAS & VPN. Additionally most computers are connected to a local (internal) network from which data can branch through multiple points to numerous destinations.

Typical network scenarios are:

- A corporate network that shares a private network with another company.
- A corporate network with Web servers located at an ISP, accessible either via dial-up or a permanent connection.
- A corporate network with dial-up capabilities.
- A corporate network with a permanent connection to the Internet.

Given this complex scenario and the many opportunities it offers for threats and breaches of security, implementing security should be a step-by-step process that starts with the primary local resource where the data is housed, continues through the intervening points, and concludes with the permanent connection to the "rest of the world." To support this step-by-step security implementation process, a suitable analysis and deployment architecture is needed.

In the GIAC enterprise network environment, decentralized, dispersed and distributed computer systems are the common standard. As the number of connections to On-site LANs (and number of LANs) expands so also are the risks due to Internet traffic. As computers and networks become more interconnected on the Internet, the threats and vulnerabilities to their operation continue to increase.

In identifying the areas of risks, it is appropriate to ask and answer the following crucial file system and network levels design/implementation questions:

- What kinds of access controls (Internet, wide area network connections, etc.) are going to be in place?
- What authentication protocols and procedures are to be used for local area networks, wide area networks and dialup servers?
- What type of network media, for example, cables, switches, and routers, are used and what type of security do they have?
- Will security be implemented on file and print servers?
- Will encryption and cryptography, Virtual Private Networks (VPNs), e-mail systems, and remote access be used over the Internet?
- What procedures will be implemented to ensure conformity with networking standards?

With the above in mind and in order to isolate points of vulnerability and hence delineate areas of risks to the enterprise, it is necessary to analyze the pattern of data flow through the network. From this perspective, there are two basic scenarios:

(i) Data stored on a computer. For data stored on a local computer, the operating system is the major provider of the necessary services for the protection task. Using these services requires that they be properly configured.

(ii) Data traveling across communication points. Data traveling between locations needs to be secured in a different way, and this often involves encryption. Generally speaking, this data is in one of two forms: data in the form of network packets coming into a system, and data that is leaving the system.

Protecting incoming data encompasses both guarding the data itself and guarding the system against threats posed by the data once it has entered the network. Protection activities include a system check to ensure that the data comes from an authorized sender and that it can perform only authorized tasks.

Protecting data that is leaving a computer involves insuring that it reaches its target in exactly the same format in which it was sent, without being changed. The session and data type, as well as data content, must be unreadable by a third party—that is, privacy must be preserved.

Data en route cannot be directly protected by services of the operating system. However, there are different technologies (protocols) available to create a tunnel between two nodes and encrypt the information. All of them have their individual limitations and the decision regarding the appropriate technology or combination of technologies needs to be well planned.

From the security perspective, there are two major issues involved in this exchange of information: (i) the data that is leaving a computer must reach the target without being read or changed before it reaches its destination and (ii) the packets that are reaching and entering a computer must be from an authorized user and their objective must be to pursue authorized tasks.

2.1.2: Risk mitigation: In a network, the ultimate burden of security falls on the operating system, although appropriate hardware support can minimize the impact of security features on network performance. Consequently, a network system that satisfies the enterprise, multi level security (MLS) policy [3] (or other policies) must enforce access control: processes from having access to objects in accordance with security policy. In addition, the network system itself must not be a channel for communication of information not in accordance with the security policy.

The response or countermeasure to potential threats involves operational requirements analysis, risk analysis, facility design support evaluation, and related access control/intrusion detection technique modeling and analysis, and the evaluation of secure

communications services and systems. Since a crucial step in IT security is the clear and unambiguous definition of specific security needs, this area must receive the appropriate emphasis and attention.

Risks reduction and elimination policies must be hard coded into the design of the network and critical systems such as the Web and SQL servers. In this regard, the architecture must incorporate the following proposed elements that in combination will provide some level of risks mitigation (Table 1).

Implementation of the multi-layer security scheme greatly reduces the risks the network faces from the Internet traffic. The scheme envisages the use of a combination of packet filters and application-level firewalls because neither the packet filter nor the application-level filters provide complimentary functions. The implementation requires the formation of security layers using packet-forwarding devices with varying degrees of packet filtering and blocking functions. The arrangement is the use of filtering routers at the perimeter of the network and application-level firewalls inside the network. Also, part of the stringent security measure is the deployment of intrusion detection systems (IDS) to detect unwanted traffic.

GIAC's "Crown Jewels"

Quality of service (QoS) is a major indicator of how well a service oriented company performs. The QoS is always adversely affected by disruptions in the delivery of service. Disruption of service leads to refunds of the fees in accordance with the length of time the disruption was in effect. Multiple disruptions lead to the subscriber viewpoint of poor service, which leads to subscribers canceling for another provider. Both issues directly hit the bottom line. Based on the priorities listed above, GIAC Enterprises has determined that **Availability/Continuity/Integrity of the service** is the most important priority.

Therefore, GIAC Enterprises has determined that the sustenance and security of the e-commerce marketing methods (e.g., Website operations and its support services) to be the crown jewels of the company. Loss of the Website may mean that financial data and customer records can't be accessed, as the Web can't be surfed. These events can mean loss of revenue, as business clients, subscribers and business partners could demand refunds, and can resort to legal actions to back up the demands. Loss of service can also precipitate negative publicity in the media, as a major outage gets news coverage, and can generate political pressure from State Attorney Generals looking to get refunds, or elected legislators calling for investigations and hearings. All of the above can have an adverse effect on the bottom line, and can drive the company out of business.

It is important to note that the Web site is hosted on the company's Web servers. Thus, ensuring that the Crown Jewel is up and running at all times is the primary responsibility of the company**.** To ensure this, the design and security policies of the company must be closely aligned with the stated objectives. In this case, the security policy must fulfill the following roles:

- Stipulate that the network and systems design must provide safeguards against discontinuity of operations due to Denial of Service attacks on the network and Web server;
- Stipulate and clearly define the policies for the management of the Web server taking into account hot patch roll out management and redundancy policies;
- Stipulate and clearly define methods of guaranteeing the integrity of data and Web site information; and
- Provide adequate mechanisms to allow only authorized clients and users into the properly designated network resources.

2.2 IDENTIFICATION OF GIAC RISKS AND MITIGATION MEASURES

From the analysis given in Sections 2.1.1, it is apparent that there are multiple areas of risk to the GIAC ENTERPRISE. The following have been identified as areas of risks to the GIAC ENTERPRISES.

2.2.1 Secured High Availability/Integrity of the service

The GIAC has to guarantee and protect the continuity or uninterrupted service and integrity of the Website operations, network service and must be able to make the operation of the network relatively secure. This extends not only to the routers and switching elements of the network but also to the protection and integrity of the service delivery host platforms, including Web servers, DNS servers, mail servers, SQL servers, and caches, and any other service platforms operated by the GIAC.

Concern: According to the CSI/FBI 2001 computer crime survey [4], Internet systems are becoming a more frequent point of attack. "For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the rise in those citing their Internet connections as a frequent point of attack rose from 59% in 2000 to 70% in 2001." – CSI/FBI 2001 Computer Crime Survey.

These attacks take different forms one of which is Denial of Service attack (DoS). If there is a denial of service attack services could be disrupted with the potential loss of service to the customers. Hence the main concern is **Denial of service attack on the network and/or Web server.**

Threat: The threats would be various points inside the IT infrastructure that are vulnerable to external including DoS attack. Everything from network, Web servers, hardware or operating system holes to application coding issues pose a security threat.

Consequences: The consequences include financial losses due to legal/regulatory or civil actions, system downtime, and loss of customer confidence. Since about 85% of our business is on-line, an outage of any magnitude causes us to loose revenue.

Risk mitigation: Create an Internet DMZ policy. This policy should, at a minimum, address the following items:

- Stipulate that the network and systems design must provide safeguards against discontinuity of operations due to Denial of Service attacks on the network and Web server. Such measures should include a provision for alternate Internet routes and Web server hot standby redundant configuration.
- Provide adequate mechanisms to allow only authorized clients and users into the properly designated network resources.
- Perform periodic firewall rule set review
- Perform vulnerability scans and penetration tests.
- Install both network based intrusion detection systems and host based intrusion detection systems.
- Define process for approval and testing of new systems or applications being placed into this environment.

*2.2.2 Client Security (*Unauthorized Access)

As well as protecting its own service assets from intrusion and disruption, the GIAC is expected to assist clients, subscribers and business partners to secure their operation from security incidents. This can take various forms, but normally does not extend all the way to have the GIAC assume all responsibility for client network security. However, in certain areas, the client must trust the company's integrity of operation in order to implement its own security policy . . .

The main issue is **unauthorized access to network resources and mission-critical devices**

GIAC ENTERPRISES is legally obligated to protect their personal and confidential information. If this is not done, an attacker may be able to gain access to confidential information from the outside world. A key element here is access restrictions and passwords rules.

Concern: The concern is that if stringent passwords and access rules are not implemented a substantial loss could be incurred by the company. GIAC needs to ensure confidentiality of its data, as well as have the ability to override any password or pass code at any time in connection with its use of its computer and electronic communications systems. Employees and authorized users should not share or use another person's password or pass code to access a file or retrieve any stored communication. The goal is to prevent unauthorized access to the firm's systems and

data by protecting the passwords and pass codes, which allow access to these systems and data.

Threat: The risk is substantially high that unauthorized system access by unauthorized persons could occur. These unauthorized persons could be either employees or visitors who have entered the facility.

Consequences: The consequences are enormous and could be any thing from SEC sanctions, loss of business, company collapse due to legal or regulatory issues, and loss of intellectual property.

Risk mitigation: Enforcement of strict password policy and other security measures including physical security should be mandatory. An effective monitoring program should be put in place including training programs that educate the entire organization on the importance of passwords security and access control methods.

2.2.3 Remote Access

Remote access is almost assured in today's e- business transactions by traveling employees and business partners there is the need to implement remote access security.

Concern: Remote access through RAS, VPN or any other technique can be used to attack or subvert the network, and mission critical systems that represent a significant investment on the part of GIAC Enterprises. As a result, GIAC needs to take certain precautions to protect the business operations.

Equally, It is important to pay attention to securing the tools used by employees to access the GIAC network from a remote location. If these tools are not safeguarded, it could leave GIAC in a vulnerable position.

Threat: The treat here is that poorly secured remote access could become a conduit pipe for attack on GIAC IT infrastructure.

Consequences*:* Using the remote access to gain a foot hold and attack the company could lead to financial losses due to legal/regulatory or civil actions, system downtime, loss of data and loss of customer confidence.

Risk mitigation: Remote access use should be limited to only those needing it for business with technical and management safeguards.

- Guidelines should be created for the use of GIAC remote access facilities. Example - Access privileges are generally only granted to managers, team leaders, associates responsible for overnight/weekend support, and sales staff.
- Employees or those requiring remote access to the network should have the approval of senior management, as well as the operation department.

- There should only be one method of connecting to the network from a remote location. IT needs to have the ability to turn remote access off at any time.
- Ensuring that proper authentication and data encryption mechanisms (e.g. VPNs) are in place should be mandatory.
- Define what type of data needs to be encrypted as well as the standard encryption techniques.

2.2.4 Executable/Malicious Code Protection

Executable/Malicious code can take many forms. ActiveX, Java applets, Viruses, Trojan Horses, and Worms are all examples of malicious code. A common misconception is that other kinds of electronic nasties, such as worms and Trojan horse applications, are viruses. They aren't. Worms, Trojan horses, and viruses are in a broader category analysts call "malicious code." There is always a deadly collateral /payload associated with each. Due to the inherent dangers every attempt should be made to check this.

Concern: Here the primary concern is **data destruction, defacements and other damages that could come from malicious code execution.**

Threat: The threat is very high because introduction of malicious codes could spell doom for the e-commerce activities. ." When loaded onto a machine, a Trojan horse can capture information from your system -- such as user names and passwords--or could allow a malicious hacker to remotely control your computer. A worm program replicates itself and slithers through network connections to infect any machine on the network and replicate within it, eating up storage space and slowing down the computer. But worms don't alter or delete files. A Trojan horse doesn't replicate itself, but it is a malicious program disguised as something benign such as a screen saver.

Consequences: According Computer Economics latest report [8], the cost of malicious code cost the world 13.2 billion US dollars in 2001. Malicious code incidents typically cost companies down time as well as technical personnel time needed to recover from the infection.

Risk mitigation: Installing a reliable antivirus scanning software. Major antivirus software vendors, including Symantec, Network Associates, Computer Associates, and Trend Micro, provide regular updates. (Computer Associates' InoculateIT is also free.) Some of the vendors also offer a service that will automatically retrieve updates for you from the company's Web site.

Regular updates are essential. Researchers at Computer Economics estimate that 30 percent of small businesses are vulnerable to viruses either because they don't keep their virus-scanning software updated or because they don't install it correctly.

Disabling Java applets and ActiveX components on the system if they are not required should be mandatory.

Table 2 below details the proposed risk mitigation measures for the GIAC ENTERPRISES.

PROPOSED SECURITY ELEMENTS OF GIAC ENTERPRISES	
Multiple Internet Access	The design incorporates two Internet routes with one as a back up
Anti Virus protection (scanning) with Real time scanning at the gateway	Scanning should also be implemented at the gateway including the firewall levels
Integrated VPN Support	The design includes a VPN server. A VPN is "a combination of tunneling, encryption, authentication, and access controls used to carry traffic over the Internet (or a managed IP network or provider's backbone). Virtual Private Networks are used to help organizations support sales over the Internet more economically--tying business partners and suppliers together, linking branch offices, and supporting telecommuter access to corporate network resources. A VPN can reduce costs by replacing multiple communication links and legacy equipment with a single connection and one piece of equipment for each location
Disaster Recovery Program	Should be implemented using effective imaging techniques such as tape backups on a rotational basis
Network- based Audit Support (scanners)	This ensures periodic assessment of the network to identify vulnerable areas
Malicious code management implemented at the firewall gateway with Options to block Java applets, ActiveX objects, unsigned software, non-commercial software and unwanted file type	This will reduce the incidence of data corruption and manipulation.
Intrusion Detection System	The use of Intrusion detection system will help to identify and in some cases prevent unwanted Internet traffic by intruders, hackers, etc.
Implementation of Multi-layer Security Scheme	The screening routers, firewalls and proxy servers will complement operating system security
Redundant systems	To effectively prevent downtime of critical systems e.g. Web servers, hot standby redundancy should be implemented in addition to RAID 5
Patches and hot fix management	There should be a program to roll out patches and hot fixes in a timely manner
Support for Multiple OS Platforms	Some operating systems are more vulnerable. For instance the Linux OS is less prune to hacking.

Table 2: Proposed risk mitigation security elements for the GIAC ENTERPRISES network architecture

3.0 ASSIGNMENT #3 EVALUATION of SECURITY POLICIES

3.1. *Evaluation of Security Policy:*

Policy: The following policy contained in **Appendix 1** is based on the policy in use at GIAC ENTERPRISES. The GIAC Enterprise policy is aimed at preventing Web server Denial of Service attack.

Evaluation: Overall, the policy is dry. The issue is that it was not written according to the standard procedure i.e. it did not specify and include any details on the following crucial sub-items of a good policy:

- Background
- Scope
- Responsibility
- Ownership
- Action

At best it contains the policy statement without any clear delineation, statements and specifics on any of the above itemized. In evaluating the above policy it is necessary to take a cure from Christopher King, et al [7], who wrote that:

"Policies are higher level documents that do not specify technologies, but focus on addressing a complete picture . . . A policy not only explains the how, but also the why, provides a stronger baseline for people to follow, and through this simple education it enables people to understand the goal of the security program."

The policy in itself contains a good policy statement on what needs to be done and why i.e. the purpose. But it does not come close as a standard policy document. The document needs to be re-written in the fashion and format prescribed by SANS [6] in order to be usable for GIAC Enterprises.

The policies are intended in a broader context to guarantee that there is a secure availability of the company's E-business transactions at all times. Specifically, two issues are covered here namely:

(i) Countermeasure against a "Denial of Service" (DoS) attack on the Web server; and
(ii) Countermeasures to prevent exploiting any operating system or application vulnerability.

Technically, in the case of the DoS countermeasure, the policy neglected the fact that the Web server could be cut off if there is a DoS attack on the network. Although the network design has provision for an alternate route the policy should specify measures to switch to the alternate route in case of an attack.

Equally, the policy was not explicit on the steps that should be taken when applying the patches and hot fixes. A specification would be beneficial.

3.2. REVISED POLICY

The original policy is contained in Appendix1

The following revision will be made in accordance with SANS format [5]

GIAC ENTERPRISES Web Server Management Security Policy

3.2.1 Background

In recognition of the fact that the GIAC ENTERPRISE Web Server is a scalable, high-availability/performance Web server, underpinning business-critical solutions for the world's leading financial news provider, it calls for a flexible Web-based management, extensive integration capabilities, and the most comprehensive range of features available that combines to provide a fully extensible secure e-commerce transactions on the Web site. Attainment of this is the driving force of the GIAC ENTERPRISES security policy.

This policy governs the management of the Web server for a watertight uninterrupted and secure operation. GIAC ENTERPRISES encourages the highest level of professionalism in the maintenance of its World Wide Web site, and this policy is intended to guide the preparation and management of the Web server security practices.

3.2.2 Purpose

The purpose of this policy is to establish standards for the base configuration of the corporate Web servers of GIAC Enterprises. Effective implementation of this policy will minimize unauthorized access to GIAC Enterprises proprietary information and technology.

3.2.3 Scope

This policy applies to the Web servers of GIAC Enterprises, and to all downstream servers associated with GIAC Web site production and operations.

3.2.4 Policy

3.2.4.1 General

- In order to ensure system-level availability of 99.999% on a 24x7 basis, two or more identical Web servers with hot standby configuration shall be maintained at all time.

- At any given time, at least one Web server should be in active production mode while the other(s) should be in passive mode in a hot standby configuration.

- General access to the Internet should always be established for business purposes only. Users are advised not to use the Internet for non-business activities in order to conserve bandwidth.

- To prevent exploitation of operating system and application vulnerabilities, the Web servers shall be updated regularly in a timely manner with the latest Service Packs, patches and hot fixes.

- The patch and Service Pack levels must be the same for all the Web servers. Application of these shall be in accordance with software vendor's defined guideline.

- It is the responsibility of GIAC Enterprises employees and other users with remote access privileges to ensure that their remote access connection is given the same consideration as the user's on-site connection to GIAC Enterprises.

- The operations department Network Security Team has the responsibility for the operation and maintenance of Internet and remote access services. In connection with this, the network security team will implement, provide, and maintain the devices and software used for the remote access services.

- Web server and network access must be strictly controlled. Control will be enforced via the use of a software client provided by network security; access will be controlled by protected password rules.

- At no time should any user provide reveal his or her login or password to anyone.

- All access to the Web servers must be done from a GIAC Enterprises provided server within the operations department. The use of personal computers on the network is strictly forbidden.

- Users with remote access privileges must ensure that their company-owned laptop computer, which is remotely connected to the network via the Internet, is not connected to any other network (i.e., home network) at the same time.

- Remote access service is restricted to authorized employees and is only to be used to access duly designated devices and services on the network.

- Non-standard hardware configurations must be reviewed, tested, and its configuration documented and approved by network security before it is allowed to access the network remotely.

- All hosts that are connected to the network via remote access must use the most up-to-date anti-virus software, and must be scanned for viruses on a duly prescribed basis.

- Operating System configuration of the Web servers should be in accordance with approved Information Security guidelines.

- Services and applications that are not required on the Web servers must be disabled where practicable.

- Access to services on the Web servers 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 the Web servers (except redundant configuration) and other 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.

- Web Servers should be physically located in an access-controlled environment.

- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

- All ActiveX and Java Applets on the Web servers should be disabled to prevent malicious code execution.

3.2.4.2 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as stipulated below:

- All security related logs should be kept online for a minimum of 4 week.
  - Daily incremental tape backups will be retained for at least 3 months.
  - Weekly full tape backups of logs will be retained for at least 3 months.
  - Monthly full backups will be retained off-site for a minimum of 2 years.
- Security-related events will be reported to Information Security Officer, who will review logs and report incidents to management. Corrective measures will be prescribed as needed. Security-related events of all kinds will be reviewed including:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

3.2.4.3 Ownership and Responsibilities

It is the primary responsibility of the Head of Operations to enforce the policies. These shall include those policies regarding availability and the management of security updates. The operations group that is responsible for system administration must own all GIAC Enterprises servers, workstations and network resources. Approved server configuration guides must be established and maintained by each group, based on business needs and approved by Information Security. Groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each group must establish a process for changing the configuration guides, which includes review and approval by Information Security.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2.4.3 Compliance
Audits will be performed on a regular basis by the external audit group from outside GIAC Enterprises in accordance with the procedures stipulated in the Audit Policy Guide.

3.2.3 Enforcement

Violation of the policies stated here will warrant corporate disciplinary action.

3.2.4 Definitions

Term	Definition
Web Server	For purposes of this policy, a Web Server is a GIAC Enterprises Server that hosts the GIAC Web site.
Patch	A patch is software installed on the Web server as a corrective action.

4.0 DEVELOPMENT OF SECURITY PROCEDURES

GIAC Procedural document

The procedure that is presented here is the procedure for establishing Web server hot standby redundancy. It ensures that:

- Two or more Web servers are on a hot standby regime,
- Only one Web server is active at a time.
- The Web servers are current with Service Packs and patches

4.1 Procedure for establishing hot standby redundant configuring on the Web servers

Background: High-availability considerations are essential operational goals. High availability is a function of the application as well as the whole network between a client

workstation and a service located in the network. While the mean failure time of individual components is a factor, network availability is determined mostly by the network design. High availability of the Web servers should be implemented with the hot standby redundancy technique.

This means that the application of design principles in the implementation of high network system availability should short circuit such issues relating to resources usage including system memory and CPU usage.

Responsibility: The network security team in the operations department is responsible for the implementation of the procedures described below.

The procedure is illustrated in the following steps.

Step 1
Configure the Web servers (four in this case) to be on a hot standby regime.

The commands in the following example configure four Web servers (Web1, Web2, Web3, and Web4) with IP addresses 208.96.22.110, 208.96.22.101, 208.96.22.102, 208.96.22.103 on a **standby configuration.**

All configurations are made at the **"**GIACWEB(config)# " prompt.

```
GIACWEB(config)# server real web1 208.96.22.100
GIACWEB(config-rs-web1)# port http
GIACWEB(config-rs-web1)# exit
GIACWEB(config)# server real web2 208.96.22.101
GIACWEB(config-rs-web2)# port http
GIACWEB(config-rs-web2)# exit
GIACWEB(config)# server real web3 208.96.22.102
GIACWEB(config-rs-web3)# port http
GIACWEB(config-rs-web3)# exit
GIACWEB(config)# server real web4 208.96.22.103
GIACWEB(config-rs-web4)# port http
GIACWEB(config-rs-web4)# exit
```

The command "server real web (x) IP address " establishes a standby redundancy
The command "port http " establishes a transmission using port 80
The command "exit " concludes the configuration.

Step 2
Establish the order of priority for switching passive Web servers into an active mode should the active server go down.

The commands in this example configure two VIPs (VIP1 and VIP2). The server-priority command in this example configures this GIACWEB to have the highest GIAC priority (255) for VIP1 and the lowest GIAC priority (1) for VIP2. Thus, this GIACWEB is the default active GIACWEB for VIP1 but is a standby GIACWEB for VIP2.

```
GIACWEB(config)# server virtual vip1 208.96.22.100
GIACWEB(config-vs-vip1)# port http
GIACWEB(config-vs-vip1)# bind http web1 http web2 http
GIACWEB(config-vs-vip1)# sym-priority 255
GIACWEB(config-vs-vip1)# exit

GIACWEB(config)# server virtual vip2 208.96.22.101
GIACWEB(config-vs-vip2)# port http
GIACWEB(config-vs-vip2)# bind http web3 http web4 http
GIACWEB(config-vs-vip2)# sym-priority 1
```

The command "server virtual vip 1 IP address " establishes a virtual IP address
The command "port http " establishes port 80 as the default transmission port.
The command "bind http web3 http web4 http" binds port 80 on the two web servers
The command "sym-priority 1" assigns the priority.

The command "exit " concludes the configuration

Configure the other GIACWEBs the same way, but give VIP3 GIAC Web server priority 1 and VIP4 Web server priority 255.

Step 3

Make sure to enter the **write memory** command after any configuration changes.

4.2 Procedure for hot patch management on the Web servers

Background: It is critical that every Web server is current on patch and Service Pack levels at all time. This is to forestall any attempt by anyone to exploit system vulnerabilities. Service Packs and hot patches eliminate the vulnerabilities. When applying a patch or patch cluster on the Web server, you must ensure that the recommended patch or cluster is installed in the order recommended by the software vendor.

Responsibility: The network security team in the operations department is responsible for the implementation of the procedures described below.

The following Steps/procedures should be followed:

Step 1

Use the command 'listrev -p' to list the patches currently installed on the Web server. All patches can be downloaded from http://Websolve.GIAC.com/patches. At that site, go to Patches>Recommended & Security Patches to see the list of Recommended & Security Patch Clusters for the Web server'.

Two numbers, for example 106125-10, identify Web server patches. The first number (106125) identifies the patch itself. The second number identifies the version of the patch (10).

Step 2
Download the appropriate patch or Service Pack

Step 3
Test the patch on the "Test sever" prior to application on the Web server to ensure that services on the server run smoothly afterwards.

Step 4
Install the latest version of the patch in order to benefit from the latest fixes.

Step 5
For any patches not found in the above cluster, please go to Patches>Patchfinder on http://Websolve.GIAC.com/patches. "

REFERENCES

1. Ranum, M., "Firewall performance measurement techniques: a scientific approach, Maximum security: A hackers guide to protecting your Internet site and network", Macmillan Computer Publishing, Chapter 27, USA. 1995.
2. Harding, H., Zhong, P., Iheagwara, C. "Optimizing the performance of enterprise networks in E-business environments", Technical document, UTV Computer Corporation, Silver Spring, Maryland, USA, June 1999.
3. Fiertag R.J., Levitt K., Robinson L. "Providing Multilevel Security of a System Design". *In Proc:* Symposium on Operating System Principles, (1977) 57 – 95.
4. Computer Security Institute, 2001 CSI/FBI Computer Crime and Security Survey. Available at http://www.gocsi.com/press/20020407.html
5. The SANS Security Policy Project. Available at http://www.sans.org/newlook/resources/policies/policies.htm
6. The SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts Consensus, Version 2.100, October 2, 2001. Available at http://www.sans.org/top20.htm
7. Christopher M King, et al, Security Architecture, Design, Deployment & Operations, 2001, The McGraw Hill Companies, pg 13
8. MalWare cost the world 13.2 billion in 2001. 2/26/02. Available at: http://www.computereconomics.com
9. SANS Information Security Officer Training Course Materials. Tyson's Corner, March 2002

APPENDIX 1 – GIAC POLICY

…GIAC ENTERPRISES Policy for Web Server DoS/Management

This policy governs the management of the Web server and is aimed at preventing a denial of service attack (DoS) on the Web servers i.e. for the **Security, Continuity/Integrity of our e-business financial data and news Web-based dissemination service.** Its aim is to provide and maintain uninterrupted and a watertight secure operation of the Web site.

GIAC ENTERPRISES encourages the highest level of professionalism in the maintenance of its World Wide Web site, and the GIAC ENTERPRISES policy is intended to guide the preparation and management of the Web server security practices such that at least two or more Web servers will be ready at all times to forestall any denial of service attack.
This includes the following policies regarding availability and the management of security updates.

***(A) High availability policy*:** In order to ensure system-level availability of 99.999% on a 24x7 basis, two or more identical Web servers with hot standby configuration shall be maintained at all time. At any given time, at least one Web server should be in active production mode while the other(s) should be in a passive mode in a hot standby configuration.

***(B) Web server updates*:** To prevent exploitation of operating system and application vulnerabilities, **t**he Web servers shall be updated regularly in a timely manner with the latest Service Packs, patches and hot fixes…