Global Information Assurance Certification Paper

GIAC Security Leadership Certificate (GSLC)

GIAC Enterprises
Fire Wall Implementation Study Overview and Recommendations

Practical Assignment
Version 2.0

"If the threat to information resources continues to expand at the current rate, many organizations will not survive five more years."[1]
~The SANS Institute~

Submitted by: Elaine Clem
September 20, 2004

ABSTRACT

The use of firewalls is an essential part of security architecture and establishing a defense in depth strategy, regardless of the size or type of organizational network being secured. The document that follows outlines the findings of recommendations from a previously conducted study featuring the use of firewalls for a global fortune cookie company that conducts its transactions via the Internet. The document evaluates aspects of the study that the author agrees with and those with which there is disagreement. Additional consideration is given to ways in which the recommended solution could be improved. While focusing on firewalls, the document also discusses the use of routers, virtual private networks, and intrusion detection systems. Also provided is a Total Cost of Ownership analysis, a Return on Investment analysis, and additional recommendations to further enhance the security posture of the company.

Table of Contents

Executive Summary

Today's electronic business environment includes a constant presence of risks and threats. We consistently hear of stories outlining loss of company assets and damage to computer networks that has resulted from viruses, worms, Trojan horses, and other types of mal-ware. As GIAC Enterprises (GIAC) has expanded operations, we have increasingly become a target of hackers. Attacks against our network necessitate the allocation of resources to assure our assets (our fortunes, customer lists, employee and supplier information and our network) and our electronic interactions with our customers, suppliers, and corporate and remote employees are secured in an efficient and cost effective manner.

Because our business model is heavily dependent upon the Internet, a study was performed to develop a firewall recommendation for GIAC. What follows is an overview of the study, an evaluation of its strengths and weaknesses, suggested enhancements to the study findings, and recommendations to proceed with the proposed firewall security architecture, including suggested changes.

The study was designed with a "defense in depth" strategy in mind. This strategy employs a strong security architecture that can withstand an attack, has many aspects and dimensions, and is based on the principles of confidentiality, integrity, and availability (CIA).[2]

It is the purpose of this document to provide support for the recommendations made by the original study prepared by Mr. Hlavac and to provide additional considerations that GIAC is encouraged to pursue. The document also includes results from a Total Cost of Ownership analysis and a Return on Investment analysis – both of which support the implementation. Additionally, a series of studies are suggested that include: conducting a vulnerabilities assessment, establishing a vendor assessment process and a related contract review, developing a data classification strategy, reviewing the existing GIAC Information Security Policy to assure alignment with recognized best practices, and developing and providing information security training to all GIAC employees.

Your review and acceptance of the recommended router, firewall, virtual private network, intrusion detection system, and anti-virus solution by October 4, 2004 will enable us to proceed with an implementation timeline aimed at having the updated system in place by the end of second quarter 2005.

By implementing a strong security architecture, our company will be viewed favorably by our customers and suppliers as they recognize our commitment to protecting the information we maintain about them, thus helping to preserve our reputation in the marketplace. We will be helping our employees better manage their daily responsibilities by reducing system down time and we will reduce unanticipated costs associated with security attacks by preventing some of them on a proactive basis and reducing the impact of those that do occur.

Study Review: Identifying a Technical Solution

A member of the GIAC Enterprises Information Technology Department accepted the task of conducting a study and recommending a firewall solution that would provide an acceptable level of security for our operations. This study can be found at:

http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf

The study encompassed the development of a defense in depth strategy, incorporating the principles of confidentiality, integrity, and availability. The defense in depth strategy focuses on implementing various layers of protection to reduce the likelihood of malicious attacks and to minimize the impact of successful attacks.

Business, User Access, and System Access Requirements

The recommendations made were based on business and access requirements. Access requirements were further distinguished between "user access" and "system access." User access refers to the "portion of the network a user needs access to in order to perform the duties assigned to that group."[3] System access refers to the access needed for the applications or systems to operate in accordance with business functions, routine maintenance, and standard network traffic."[4] The specific requirements outlined in the study are below.

Business Requirements[5]:

- Customers need to access the web servers to purchase fortunes.
- Suppliers need to access the network to provide fortunes to us.
- Tele-workers and our mobile sales force need the same access as on-site employees with the same level of relative security.
- The various systems need access to each other.

User Access Requirements[6]:

Group	Access Needed and Explanation	Port(s)
Retail and Wholesale Customers	Outward facing content web server to access information on web servers to produce sales leads	80, 443
	Outward facing retail purchase web server for ordering fortunes from the web servers	80, 443
	Outward facing e-mail server to e-mail questions or comments to the company	110
Business Partners	Outward facing content web server to access information on web servers to produce sales leads	80, 443
	Outward facing e-mail server to e-mail questions or comments to the company	80, 443

	Outward facing File Transfer Protocol (FTP) server to send and receive bulk fortunes via a secured means with all files requiring Pretty Good Privacy (PGP) or GnuPG (GPG) encryption	20, 21
Tele-Employees, Mobile Sales Force, and Corporate Employees	All employees would be given equal rights to all network components with authorization granted at the operating system or application level	50, 500

System Access Requirements[7]:

System	Access Needs	Port(s)
Web Purchase Server	Microsoft Transaction Servers (MTS) using XML to post to the Internal MTS server using SSL – the MTS server(s) will make the necessary calls to the customer and fortune databases	443
External/Internal FTP Servers	Internal File Transfer Protocol (FTP) servers are needed to pull and push FTP files to the external FTP servers – only those files with .asc extensions (PGP/GPG text versions) will be transferred	20, 21
Support Systems	Support systems, such as the Domain Name Service (DNS) system, will need access to various parts of the network to support proper domain naming conventions	53
Supplier Network(s)	External FTP servers are needed for suppliers to send FTP files to – each supplier will have a separate log-in account and is required to send all files in the PGP/GPG format	20, 21
Virtual Private Network (VPN) Access	All tele-worker's systems will need access to the internal network	50, 500
Lightweight Directory Access Protocol (LDAP)	Utilized to access and update information in a directory.[8]	389

Recommended Architecture

Based on scenario testing performed during the study, it was recommended that GIAC use of a four router, dual firewall architecture with Intrusion Detection Systems (IDS) located at three points in the network. The recommended firewall solution is configured to include a Virtual Private Network (VPN).

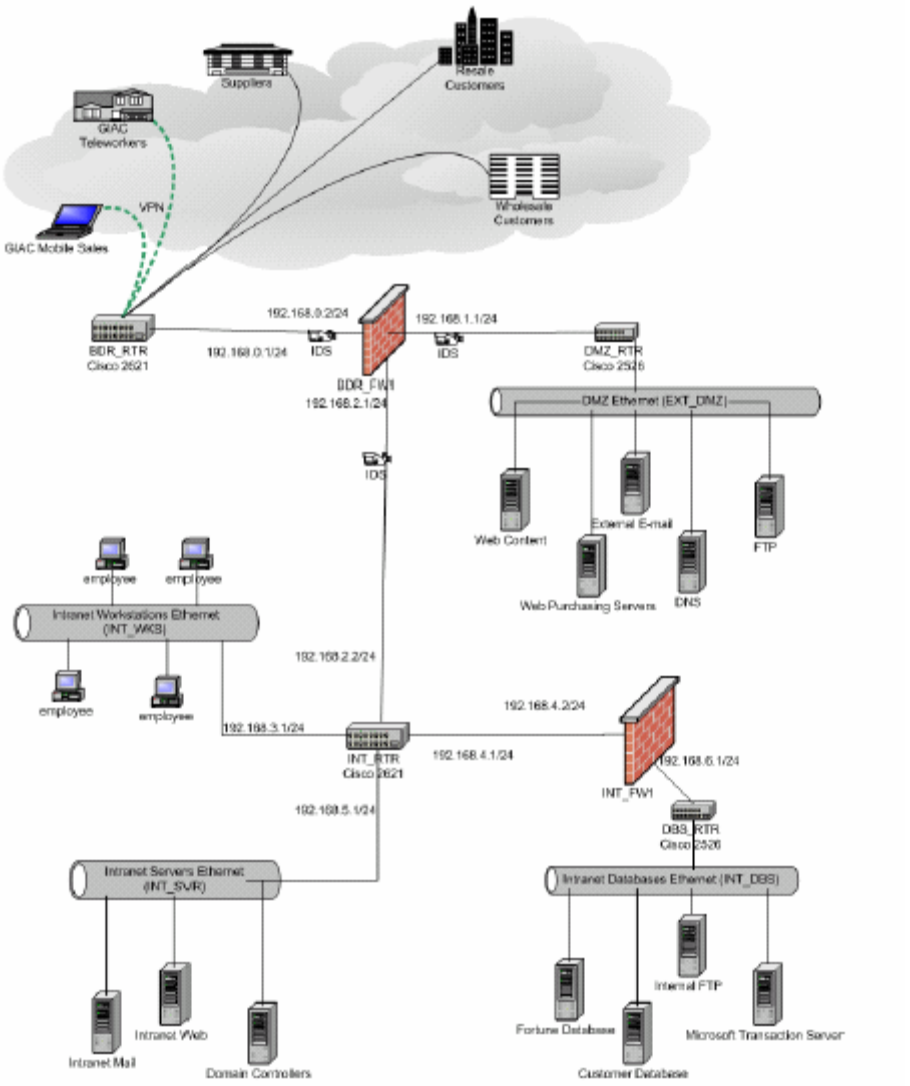

Figure 1: Dan Hlavac Network Design (page 49)

The border router (BDR_RTR) serves as the "basic traffic filtering"[9] device and directs data packets from the Internet to an IDS (BDR_IDS) and the border firewall (BDR_FW1) through a second IDS (the DMZ_IDS or the INT_IDS) and then on to either the DMZ router (DMZ_RTR) and DMZ Ethernet (EXT_DMZ) or an internal IDS (INT_IDS) and internal router (INT_RTR). Data packets that clear the internal router are directed to one of three subnets. The subnets are represented as the Intranet Workstation Ethernet subnet, the Intranet Servers Ethernet subnet, and the Intranet Database Ethernet subnet. Note that the original study recommendations did not include the use of IDSs; however, subsequent testing suggested this added measure of securing our network was appropriate.

The Intranet Workstation Ethernet subnet is utilized by employees accessing the Intranet to perform their daily job duties. The Intranet Servers Ethernet subnet supports the Intranet Mail, Intranet Web, and Domain Controller Servers. Unlike the other subnets, the need to maintain additional protection for the company's assets (fortunes), customer information, a secured means of exchanging file information (via FTP), and the web purchase servers used to collect customer orders was recognized. To fulfill this need, an internal firewall (INT_FW1) was recommended. A fourth router (DBS_RTR) was recommended to enhance the efficiency of the database subnet.

Routers

The study initially recommended the use of two Cisco 2621 Routers running on an IOS 12.2(8) operating system and using Cisco's Extended Access Control List. After testing, the addition of two Cisco 2526 routers was suggested. A summary of the border router configuration is provided below; however, if the reader would prefer to see the suggested program code, please view pages 13-16 of the study.

The border router configuration is arranged in a manner such that "Cisco's state-full packet filtering allowing return packets from established sessions"[10] is enabled. A review is not conducted for packets without an IP name. Packets with an IP name will be reviewed by applying numerous protocols, including: TCP, UDP, HTTP, HTTPS, FTP, SMTP, and TFTP. Fast Ethernet, a LAN switching product, is used to determine if the packet will access the router for further direction within the public or private network sections.

Access Control Lists are used for "screening incoming traffic for validity (anti-spoofing), screening the destination addresses of traffic within the *network*, and to the extent possible, restricting *network* services visible to the remainder of the enterprise to the set of intended services."[11] Access Control List 100 is configured to allow all outbound traffic from valid networks. Incoming access requests reviewed by the Access Control List 101 configuration will stop packets attempting to access private IP addresses and will allow WWW, SMTP, FTP-data, port 53, port 500, and port 443 access requests to be directed by the border router. All other traffic will be denied access.

Static routes are allowed for a series of Class C internal subnets. A warning message was developed to advise that "unauthorized access to the (*internal subnet*) device is prohibited."[12]. Additional commands were included to enable SSH connection time-outs, "to minimize the risk of an attacker uncovering certain information about GIAC's network," to "help prevent ICMP messages from disclosing GIAC's network information," to encrypt the configuration file password, and to help protect GIAC from Denial of Service attacks.[13]

Access Control Lists were also suggested for the Internal Router. These Lists are configured based on the following requirements[14]:

- Allow all outgoing requests from the Workstation network
- Deny all incoming requests to the Workstation network
- Deny all outbound requests from the Intranet Server network

Specific configuration requirements for the DMZ router and the DBS router were not included in the study, but will need to be developed.

Firewalls

The study recommended the use of Check Point Firewall 1 running on the VPN-1/FireWall-1® SmallOffice™ operating system and using the Check Point Policy Editor to configure the firewalls. Both the border firewall rules and the internal fire wall rules are available for review on page 18 of the study.

Twelve rules were identified, but not all rules apply to both firewalls. Instead, the study emphasized that administrators should take the appropriate steps "to apply rules only to the desired firewall"[15] and to "put the most frequent requests at the top to increase process time."[16] (The author believes the study intended to say that by putting the most frequent request at the top, process time per packet review would be reduced, rather than increased, as the applicable rule would be applied in a shorter time frame.) For ease of review, please see Figure 2 for a reproduced version of the Check Point FireWall-1 Access Control List.

Rule No.	Source	Destination	IF VIA	Service	Action	Track	Install On	Time	Comments
1	*Any	GIAC_Ext_Web_Content	*	TCP http	Accept	None	GIAC_BDR_FW1	*	Anyone can access the external content web servers in the DMZ.
2	*Any	GIAC_Ext_Web_Purch	*	TCP https	Accept	None	GIAC_BDR_FW1	*	Anyone can access the external purchasing servers in the DMZ.
3	IP GIAC_Supplier1_IP IP GIAC_Supplier2_IP	GIAC_EXT_FTP	*	TCP ftp	Accept	Log	GIAC_BDR_FW1 GIAC_INT_FW1	*	Suppliers can login to Enternal FTP (DMZ) server.
4	GIAC_INT_FTP	GIAC_EXT_FTP	*	TCP ftp ?? AH	Accept	Log	GIAC_INT_FW1 GIAC_BDR_FW1	*	Allow batch process to PULL files from External FTP server to Internal FTP server. This happens once per hour and should be logged.
5	GIAC_Ext_Web_Purch	GIAC_INT_MTS	*	TCP https	Accept	Log	GIAC_INT_FW1 GIAC_BDR_FW1	*	Customers buy and sell fortunes over an SSL tunnel to the Internal Microsoft Transaction Server.
6	GIAC_Internal_Mail GIAC_External_Mail	*Any	*	TCP smtp	Accept	None	GIAC_BDR_FW1 GIAC_INT_FW1	*	Allow E-Mail.
7	GIAC_INT_WKS	*Any	*	TCP https TCP http	Accept	None	GIAC_BDR_FW1 GIAC_INT_FW1	*	GIAC Intranet employees can go to any server on port 80 or 443.
8	GIAC_INT_WKS	*Any	*	TCP SSH	Accept	Log	GIAC_BDR_FW1 GIAC_INT_FW1	*	GIAC Intranet employees have full access to all servers but it will be logged.
9	GIAC_DMZ	*Any	*	*Any	Drop	Alert	GIAC_BDR_FW1	*	All other outbound DMZ requests should be dropped with an alert.
10	*Any	GIAC_BDR_FW1	*	NBT	Drop	None	GIAC_BDR_FW1 GIAC_INT_FW1	*	Drop NetBios traffic which is not used on this network.
11	*Any	*Any	*	*Any	Drop	Log	GIAC_BDR_FW1	*	Drop but log all other traffic to the External Facing Firewall.
12	*Any	*Any	*	*Any	Drop	Alert	GIAC_INT_FW1	*	Drop but ALERT all other traffic to the Internal Firewall.

Figure 2: Reproduced from FireWall-1 Rules in Dan Hlavac's Study (page 18)

The following information is a summary of the logic used in formulating the firewall rules outlined in Figure 2. The explanations are based on information from pages 18 to 20 of the Hlavac study. Rules 1 through 8 are "allow" rules, while Rules 9 through 12 are "drop" rules that disallow traffic.

- Rules 1 and 2: Both rules are intended to allow customers to access the web content and web purchasing servers located in the DMZ Ethernet. Customer orders will be placed via a Secure Sockets Layer (SSL) connection via TCP 443, utilizing HTTPS. Customer credentials are addressed in Rule 5.
- Rules 3: This rule enables supplier delivery of fortunes via access to the DMZ Ethernet External FTP Server. Suppliers are required to provide lists via encrypted files using Pretty Good Privacy (PGP) or GnuPG (GPG) public key encryption tools.
- Rule 4: Rule 4 was included to "allow the Internal FTP server (located in the Intranet Database subnet) to call the External FTP server"[17] for batch processing of the fortunes.
- Rule 5: This rule enables GIAC's customers to purchase fortunes by allowing the External web purchasing server mobile sales force to place customer orders to the Internal Microsoft Transaction Server.
- Rule 6: Rule 6 "allows the e-mail servers to call almost anyone if it's e-mail traffic. Note this rule is NOT applied to the Internal Firewall. There is no reason to have e-mail traffic to or from the Intranet Database region."[18]
- Rule 7: This rule enables internal workstations using HTTP or HTTPS to access any server without logging.
- Rule 8: Rule 8 enables internal workstations using SSH to access any server; however, unlike Rule 7, logging will occur.
- Rule 9: This drop rule is designed to send an alert if undefined traffic is generated from within the DMZ. The intent is to identify server compromises
- Rule 10: Rule 10 drops any NetBios traffic that is not used on the network.[19]
- Rule 11: This rule will log all traffic to the Border Firewall and will then drop the traffic.
- Rule 12: This rule will send an alert for all other traffic accessing the Internal Firewall. The traffic will then be dropped.

The study provides additional detail regarding the development of the firewalls using the Check Point Policy Editor tutorial. Information outlined includes adding or inserting a standard security rule, establishing source and destination selections, selecting communication routing, identifying the service options to be used, determining what action should be taken with regards to the various data accessing the firewall, establishing track capabilities, selecting which firewall the rule is intended for, determining when each rule is applied, and inserting free form comments. While not described in detail here, screen shots and additional

information about each of the above steps are available in the study documentation found on pages 21 through 30.

Virtual Private Networks (VPNs)

The business model GIAC Enterprises has chosen includes tele-workers and a mobile sales force. In order to enable these employees to communicate with our network, a Virtual Privacy Network (VPN) was recommended. "The VPN allows a trusted network to communicate with another trusted network over untrusted networks such as the Internet."[20] To reduce incompatibility issues with the firewall, the study recommended that Check Point VPN client VPN-1 Secure Remote initiated at the border firewall be utilized.

GIAC uses a 56k dial up which is supported by the Check Point VPN.[21] The VPN will allow dial up access (GIAC's standards are set at 56k) and high speed connections, such as DSL or cable modems.

The study recommended that the VPN configuration include two password authentication methods (S/key password and the VPN-1/FireWall-1 password) and the ISAKMP/Oakley or IKE protocol that uses a triple data encryption standard (3DES) algorithm with certificates.[22] The study pointed out that VPN-1, as configured by the Check Point Gateway, includes functionality to support network address translation which is performed at the internal firewall.[23]

Intrusion Detection Systems (IDSs)

The use of Intrusion Detection System devices was not initially endorsed by management and was, therefore, omitted for the most part from the study. However, following the scenario testing, it was recommended that IDSs be used as a means to further secure the GIAC network. For this reason, it was included as shown in Figure 1 above, and will be further discussed in the following portions of this document.

Customer and Supplier Communications

Retail and wholesale customers would not use a VPN, but rather Secure Sockets Layer (SSL) protocol to place orders via the Internet in a secured manner. Suppliers would use FTP files to transmit lists of fortunes to GIAC Enterprises. The FTP files would be required to be encrypted using PGP or GPG format. Acceptable FTP files would be routed to the external FTP server located in the DMZ. The fortunes would be transferred via a job initiated by the internal FTP server to migrate the fortunes into the internal database zone.

Implementation Testing/Auditing

The next step outlined in the study was to develop a firewall implementation test/audit (note this is not the equivalent of a vulnerability assessment or a penetration test). Testing was anticipated to require a three hour window of time. In order to reduce the impact of unplanned results, the testing was planned to occur during a time that typically has low system traffic and during which regular system maintenance was scheduled. A time targeted was Sunday morning between 1:00 am and 4:00 am.

The recommended test/audit approach consisted of running a series of transactions through the system to establish a baseline standard. The firewall test cases were then processed, followed by another series of transactions to determine changes from the original baseline standard. The study included a series of eight tests. Each test was carefully monitored and documented, with necessary action items and/or issues noted for action plan development.

The tests checked the operability of fire wall rules one through four and six through nine. Rules five, ten, eleven, and twelve were not tested. Of the rules tested, rule six failed, as did the VPN client test. The failure of rule six prompted the recommendation to add rule to allow outgoing SMTP (simple mail transfer protocol) requests from workstations. The VPN test found that tele-workers and the mobile sales force did not have access to the network. This led to the recommendation of a new rule for the border firewall

Prior to testing, it was discovered that rule nine required adjustment. The rule was changed to read as shown below and resulted in a successful test.

Rule No.	Source	Destination	IF VIA	Service	Action	Track	Install On	Time	Comments
9	GIAC_DMZ	GIAC_ISP GIAC_INT_FW1	*	DNS	Accept	None	GIAC_BDR_FW1 GIAC_INT_FW1	*	DNS entry

Figure 3: Reproduced from Dan Hlavac's Study (page 47)

Another action item associated with email was identified during testing. Testing found that a rule was needed for Lightweight Directory Access Protocol (LDAP) traffic. As LDAP is not defined within the study, it will be defined here for the reader's benefit. LDAP is "an Internet protocol that email programs use to look up contact information from a server."[24]

The study also documented a test scenario in which a GIAC holding company's system was attacked using "white hat hacking." "White hat hacking" refers to hacking performed as a means to identify potential weaknesses before a "black hat hacker" with intent to cause damage identifies and exploits the weakness. A perimeter fire wall attack, an internal system attack, and a distributed denial of service attack were waged against the holding company. While permission had been received to conduct the attacks, the holding company staff was not advised of when or how the attacks would occur.

In the scenario, Cybercop Scanner software was used to conduct open port scans and social engineering was used to try to gather information. The fire wall attack was not successful because the system administrator had applied upgrades, patches, and hot-fixes in a correct and timely manner.

Cybercop Scanner and Nmap were used to conduct the internal system attack. The attack was to include installing NetCat on the holding company system to allow unauthorized remote access. This attack was not successful because TFTP rules were in place.

The Tribe Flood Network 2000 (TFN2K) daemon was used for the distributed denial of service attack which used fifty "zombie" host systems. The attack was successful and prompted the study to reference potential means by which to defend such an attack. To review the specific defensive posturing referenced by the study, please see pages 63-64.

Areas of Agreement

The study summarized above places significant emphasis on utilizing a defense in depth strategy as noted by the layering of security solutions to prevent and mitigate attacks. This approach is consistent with GIAC's security strategy. Points of agreement and the reason for supporting the recommendations made in the study are provided below.

Recommended Architecture

The recommended architecture presented by the study is considered sound and capable of achieving the defense in depth strategy GIAC has outlined. As suggested by The SANS Institute, a network's design should "publish separate mail, web and DNS servers to the Internet; provide appropriate access from the internal network to the Internet; and protect the internal network from external attacks."[25] The network architecture shown in Figure 1 provides for each of these objectives.

The DMZ allows the web content, external e-mail, and DNS servers to be accessed from the Internet. The internal network is allowed to access the internet via network address translation (NAT) active on the internal firewall and also available as a feature of the recommended routers. And, the Intranet servers and the Intranet databases are protected from external attacks via layered routers, firewalls, and intrusion detection systems. Various encryption methods are also deployed, for example, PGP, GPG, and 3DES; and secured channeling is used, for example, SSL and ISAKMP/Oakley (IKE). These efforts are reinforced by password requirements such as S/key and VPN-1/FireWall-1 passwords.

Additionally, it is worth mentioning that the component naming scheme was well thought out and easy to follow. Use of consistent and logical names such as BDR_FW1 (Border FireWall1) and DBS_RTR (Database Router) are clearly understandable and would allow for expansion as GIAC grows its enterprise network with a minimal number of architectures.

Research conducted via the Internet suggests the selection of vendors utilized in the initial study was based on sound judgment. Cisco, HP/Compaq, Microsoft, and Check Point are all reputable companies that have fared well in the marketplace. These vendors also have a global presence and scalability – characteristics that are consistent with the goals of GIAC.

Routers

While not explained in the study, the selection of Cisco 2621 routers, each with an IOS 12.2 operating system was a good choice for GIAC (even though the model is currently being replaced by the 2621XM model). The Cisco routers are

recognized for their stability, varied features, scalability, ability to be upgraded, versatility, and their overall quality. They support virtual private networks, an important consideration based on our use of a mobile sales force and tele-workers. Additionally, Cisco provides various support options via their SMARTnet service pack programs[26] – this may be helpful at least initially to assure our technicians are familiar with the routers and their related programming and connectivity.

Following testing, the study recommended the addition of two Cisco 2526 routers. The principle of adding the routers is acceptable; however, information about the chosen model was not available via the Internet. It is presumed that the Cisco 2526 model is no longer available and should instead be replaced with a different model (possibly a 3660 series model) that would achieve a similar outcome.

Firewalls

The basic premise of a firewall is to allow only the appropriate traffic in and out of the network it is installed on. The Check Point FireWall-1 firewall recommended by the study is well suited for GIAC's needs in this respect and operates in a complementary manner with a Virtual Private Network (VPN-1). The Check Point firewall is attractive for a number of reasons that are outlined here, including[27]:

- Integrating both network-level and application-level protection via the use of INSPECT, an "adaptive and intelligent inspection technology." Detailed information regarding the network-level and application-level protection offered by Check Point is available at: http://checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf
- Using stateful inspection to evaluate packet header information, like a packet filter firewall, and to evaluate the content of the data.
- Enabling the integration of multiple authentication tools.
- Deploying SmartDefense™ logic and Application Intelligence capabilities. SmartDefense™ logic to "automatically block and log oversized packets, SYN floods, and fragmented attacks." Application Intelligence "enables access control to specific HTTP, SMTP, or FTP resources based on source, destination, user privilege and time of day."
- Enabling centrally managed Check Point Security Management Architecture (SMART) solutions that allow restrictions to browse or publish documents to a specific server.
- Including status and auditing capabilities that "provide real-time geographical tracking, monitoring, and accounting information for all connections logged by FireWall-1 gateways." These tools also monitor administrator responses to situations, allowing GIAC to identify better response procedures for future attacks and to enhance the training of their system administrators.

As shown in the study, FireWall-1 can be implemented and maintained to appropriately reflect GIAC's security policies. Filtering is applied to both incoming and outbound traffic, ingress and egress filtering respectively.

The Check Point Policy Editor tutorial referenced in the study provided reflects the relative ease of using this firewall solution once there is a sound understanding of the existing network. It also allows the user to establish rules that are explainable and supported by company needs and policy.

The study has also identified good firewall placement within the security architecture. This allows separation of the semi-public network (the DMZ Ethernet) and the private network. The addition of an internal firewall within the private network to protect the Intranet Database Ethernet network enhances the security of the architecture and is representative of the importance GIAC places on our fortune database, our customer database, our internal FTP server, and our Microsoft Transaction Server.

Virtual Private Networks (VPNs)

The study recommended the use of a virtual private network through which the company's remote sales force and teleworkers could "safely" communicate with the GIAC network. As indicated above, the selection of the VPN-1 product, which complements the FireWall-1 product, is a favorable selection. The dual password requirement, including a one-time use S/key password and the FireWall-1/VPN-1 password, provides an appropriate level of password security when transmitted using ISAKMP/Oakley (IKE).

IKE provides a means of obtaining "agreement on which protocols, algorithms, and keys to use (negotiation services) to ensure from the beginning of the exchange that you're talking to whom you think you're talking to (primary authentication services), managing the keys after they've been agreed upon (key management), and exchanging those keys safely."[28] In this case, the agreed upon encryption algorithm is triple data encryption standard, or 3DES. While 3DES is considered to slow the system because it requires a longer key and three rounds of encryption, it is currently the preferred encryption standard as it has not been cracked and it can be used to combat brute force attacks (testing possible keys until the correct one is found) and "meet-in-the middle" attacks.[29]

Intrusion Detection Systems (IDSs)

Initial recommendations of the study intentionally excluded the use of Intrusion Detection Systems as directed by management; however, upon testing, it was found that the use of IDSs to monitor network activity would be beneficial in strengthening GIAC's overall network security architecture and would reinforce the defense in depth strategy GIAC policy prescribes.

IDSs are helpful tools to use in conjunction with firewalls and other security applications and techniques. As diagramed in Figure 1, it appears the recommended solution would be to use network IDSs (NIDS) to identify and send alerts for network irregularities. While in agreement with the addition of IDSs to the GIAC system, a more complete solution may be available via the use of a combination approach utilizing both network and host intrusion detection systems. This possibility will be evaluated further in the section titled "Additional Considerations."

Customer and Supplier Communications

As indicated in the study, customers and suppliers would not have the ability to use the virtual private network to communicate with GIAC in a secured manner. Instead, for customers to receive information about the company, to place an order with the company, or email the company with questions, no encryption method is specified. Suppliers would need to send files to the external FTP server using a 128-bit key secure sockets layer protocol with PGP or GPG public key encryption (also at 128-bits). This is acknowledged as an industry standard.

Contacts made by both customers and suppliers would be directed to the GIAC DMZ (semi-private zone), rather than being sent directly to the Intranet database subnet located in the private zone. Internal processing is used to communicate the customer order and files containing fortunes.

The segregation of the DMZ and the Intranet database subnets, with specific call requirements for the two subnets to communicate, provide additional protections to the GIAC network. It becomes more difficult for an attacker to gain access to the private subnets based on this approach, due in part to the additional router, firewall, and IDSs that must be passed through and, in the case of suppliers and partner companies that translate fortunes, because of the additional steps taken to require separate logins for each and the steps taken to encrypt files (using PGP or GPG) moving between the external FTP server and the internal FTP server.

Implementation Testing/Auditing

Testing of the firewall rules appears to have achieved its goals. In this specific series of tests, two main weaknesses were encountered and corrected and a separate finding, the need for LDAP, was recognized and a rule was added. Use of the Check Point FireWall-1 device which utilizes the Check Point Policy Editor enabled these adjustments to be made with relative ease. This is reflective of one reason why this particular product is a top seller in the firewall market.

Areas of Disagreement

The recommendations provided by Mr. Hlavac's study are, for the most part, viewed favorably in their support of GIAC's security policies and its defense in depth strategy. However, there are areas that could be improved upon. These points of concern are reviewed in this portion of the document.

Business, User Access, and System Access Requirements

With regards to Business Requirements, the study indicated "the tele-workers and mobile sales force *would* need the same access as on-site employees with the same level of relative security."[30] While this approach helps to reduce the likelihood of encountering the "Snowflake Syndrome,"[31] there is greater security in establishing user access variations, such as that associated with separation of duties, role based access, and least privilege access.

Separation of duties refers to the process of dividing responsibilities so as to allow a check and balance approach. An example would be having one person process electronic bank deposits and another balance the account into which the deposits are made. In this scenario, by dividing responsibilities, the company reduces the likelihood of an employee embezzling company funds.

Role based access refers to the establishment of access to specified systems based on the job responsibilities of the individual. For example, a mobile sales person would have different access needs than someone working in the GIAC accounting unit. Arranging access based on the roles of employees helps to assure a "least privilege" approach is adhered to. Least privilege access is defined as limiting access to only that needed by an individual to perform their job duties. For example, a mobile sales person would have access to their own production reports, but not the production reports of another mobile sales person.

Routers, Firewalls, and Virtual Private Networks (VPNs)

To strengthen the validity of the study's recommendations, it would have been helpful for its author to include reasoning as to why the specific models were selected. However, such explanations were omitted.

While the author is in agreement with the selection of Cisco routers, discussion as to the attributes that led to this selection or a comparison of the various router products evaluated would be a beneficial addition to the study. A discussion of the features offered by each product would allow for the examination of which characteristics would be considered to be "must haves" versus "should haves" and "nice to haves." This would contribute to the development of a cost evaluation that was also lacking in the study.

Additionally, with regard to the routers, the configuration for the border router was well defined in the study, but information regarding the configuration of the internal routers was limited. Expanding upon this information would have strengthened the study.

The Check Point FireWall-1/VPN-1 product that was selected is the top seller in the market, and as indicated above, provides many positive features. Again, the original study would have been enhanced by including an explanation of why the FireWall-1 product was selected over a Cisco PIX firewall, for example, and why a different VPN was not selected.

As with the router, there was only a limited statement regarding the pricing of the FireWall-1/VPN-1 product. With the recognized importance of balancing the risk we accept with the cost we pay and the level of protection we receive, this would appear to have been logical information to include; however, the study fell short in this respect. As a result, additional pricing information is provided in the following portion of this document.

In accordance with the role based access outlined above, FireWall-1 Rule 7 could be altered to allow only that access which is determined necessary for the given job duties. As established by the study, tele-workers and the mobile sales force would be given access to the GIAC network on a carte blanc basis.

The recommended architecture indicates the use of Network Address Translation (NAT) – an "Internet friendly" way to access the Internet. NAT "enables many more computers to participate in the public Internet than available addresses would otherwise allow and provides a degree of privacy regarding *GIAC's* internal network structure.[32]

While NAT can be utilized on a number of devices, placement on the internal firewall/VPN appears to be the suggested location in the recommended architecture. Because NAT is typically used for outbound Internet calls and the internal firewall is located between the internal router and the Intranet database, it would seem more appropriate to apply NAT at either the border firewall or the internal router. This supports Internet requests being made from the Intranet Workstation Ethernet.

Intrusion Detection Systems (IDSs)

While initial plans did not include the use of Intrusion Detection Systems in the security architecture for GIAC, scenario testing found that GIAC would benefit from this additional layer of security. At that time, discussions should have taken place with management to determine the appropriateness of adjusting the scope of the study to include IDS options. This discussion did not take place. As a result, the recommendation to incorporate IDSs into the architecture lacks

support – use of IDSs was incorporated in to the study reviewed above based on the post-testing recommendation.

Additionally, as indicated in the suggested network diagram (Figure 1), the selected intrusion detection systems were to be network IDSs. As there was no explanation provided regarding use of IDSs, the reasoning for this selection was not provided. Upon review of numerous network and host IDS products available, it appears more appropriate to use a blend of network and host IDSs.

The unplanned addition of IDSs to the network was also apparent in the lack of adopting an appropriate naming scheme. The study could have easily adopted a naming scheme for the three network IDSs shown in Figure 1 above. For example, BDR_IDS, DMZ_IDS, and INT_IDS1, for the border IDS, DMZ IDS, and first internal IDS, respectively, could have been applied.

Customer Communications

The study mentioned the need for customers to have credentials to place orders for fortunes, but failed to recommend a secured solution for this purpose. Based on the volume and size of customer orders, it would stand to reason that there are expectations that a secure mechanism is in place to protect credit card numbers, bank account numbers, FEIN numbers, etc that may be necessary to conduct business. The credibility of the study would have been strengthened by including consideration for securing these communications.

One possible solution that could have been evaluated would be the use of the Secure Electronic Transaction (SET) protocol. "SET allows customers to make credit card purchases over the Internet without giving their numbers to the merchants. Instead, SET relies on digital signatures to authorize the purchase and verify that the customer's account is in good standing, with adequate available credit."[33]

SET is viewed as a positive solution for transacting business over the Internet because it helps to achieve confidentiality, integrity, and authentication of transactions.[34] The protections SET provides encourage compliance with laws and regulations, such as California Civil Code 1798.29 which requires companies that experience a breach of information, including the name and address and one of the following: driver's license number, account number, or Social Security Number, to notify those impacted by the breach, unless the information is encrypted.[35] Notification of this sort to GIAC's customers would likely be very damaging to our brand and our reputation and there may be an associated loss of business that results.

Implementation Testing/Auditing

Each of the routers, firewalls, and virtual private network mentioned above will create logging reports; however, the study made no reference to customization of the reports, who should review the reports, how frequently the reviews should be conducted, or how the logs should be protected. Establishing such guidance would prove helpful in the evaluation of the recommended solutions. If appropriate flexibility is not available, another solution/vendor may be more appropriate. While this appears unlikely based on the selections made, a reader of the study would not have any way of knowing this.

The study also failed to provide an outline of the recommended procedures that should be followed in the event an attack is logged. And, did not suggest the establishment of a review and update process to confirm that the Access Control Lists (ACLs) being utilized were properly synchronized with GIAC's information security policies.

It would also have been beneficial to include discussion regarding the importance of being vigilant in the application of updates, patches, and hot-fixes. With the exception of this importance being highlighted in the test against the GIAC holding company, this was omitted from the study.

There would also be benefit in utilizing the Cybercop Scanner against GIAC Enterprise's own system, rather than that of the GIAC holding company. It is presumed that the two companies have separate systems, each with their own idiosyncrasies. As such, an attack that failed at one of the companies may be successful at the other and vice versa. While there are lessons that can be learned from conducting the "white hat hacking" exercise against another company, the true benefit would come from applying the same approach against GIAC's own network.

One additional area of concern is the lack of reference to possible back-up systems should an attack disable a portion, or all, of the network. It makes good business sense to have such a plan in place so that normal operations may presume as quickly as possible following an incident. This should also be outlined in the Information Security Policy maintained by GIAC.

Additional Considerations

Vulnerability Assessment

The study outlined above was intended to focus on strengthening the firewall strategy of GIAC. While the study provides some evaluation of other aspects of GIAC's security architecture, a complete analysis of the network would be beneficial to identify vulnerabilities that exist, some of which may be at least mitigated by some of the solutions being outlined in this document. Prior to conducting such an assessment, it would be helpful to identify what is most important for GIAC to protect from an information security standpoint.

A likely place to start is to evaluate where GIAC places the most emphasis in terms of securing its network - protecting the confidentiality, integrity, or availability (CIA) of the system.[36] For example, is it most important for GIAC to protect the information we obtain about our customers, suppliers, other business partners (fortune translators), and employees; or, are we more concerned about the accuracy of the information we have and the prices we post for fortunes on our web content server; or, is the availability of our website the most important thing we need to secure. While each of the aspects of CIA is important, because GIAC operates as an e-business, availability of our web content and web purchasing servers is perhaps the most critical consideration.

With emphasis placed on the availability of our system, we can take steps to further evaluate methods that will enable GIAC to maintain our web site and web ordering process. This evaluation can be performed by conducting a vulnerability assessment. Application of the OPSEC Vulnerabilities Assessment process would help to drive out additional areas of concern. Such an assessment keeps cost considerations in mind as it can be conducted as an internal evaluation of vulnerabilities.

The OPSEC Vulnerabilities Assessment includes a six step process, including[37]:

- Identifying critical information
- Assessing threats or risks of the company
- Assessing vulnerabilities of the critical information by the threat
- Conducting a risk versus benefit analysis
- Implementing appropriate countermeasures
- Repeating the process

A discussion regarding the application of the OPSEC Vulnerabilities Assessment for GIAC is included in Appendix A.

Vendor Assessment and Contracts

The selection of a hardware or software vendor typically has a lasting impact on the company. As GIAC takes steps to enhance our system security and

contemplates establishing new vendor relationships, it would be beneficial to establish procedures regarding the use of a vendor assessment tool or tools. This tool could be as easy as establishing a check list of things to do once a need is identified. For example, the check list might include conducting an Internet search for potential products and vendors, checking with vendors currently used to determine if they may have a product or service that would suit your need, listing product specifications, evaluating the products ability to integrate with existing products, outlining the scalability of the product, identifying the types of service contracts that are available, conducting a price comparison, meeting with prospective vendors, and asking the security staff for their input.

A more formalized approach is known as the Analytical Hierarchy Process (AHP). This approach would allow GIAC to identify key characteristics they are looking for and to prioritize each characteristic, resulting in a weighting of each of the characteristics. Each vendor/product, though not offering the same products or services, is evaluated against the hierarchy to develop a score. While one vendor may score well in one area and not in another, their final score may be higher than another vendor that scored higher in two areas that were of lesser priority.[38]

While not the "end all, be all" of selecting a vendor, applying this procedure to our current situation as a portion of the overall vendor evaluation process, may provide additional support for the vendors recommended in the study or may lead to the selection of other vendors that were previously overlooked. It may also help the organization to prevent becoming "widgetized" by accepting new products that may not be in the best interest of the company from a long term perspective.

Once a vendor is identified and they have been thoroughly researched and evaluated, GIAC should have standardized contract language available for use in the negotiation process. For example, we may want to include a confidentiality clause that indicates information received from GIAC may not be used for any other purpose than to provide the service indicated in the contract. It would be beneficial to include service level agreements and ramifications if the agreements are not upheld so expectations for both GIAC and the vendor are understood. There are other aspects of our existing contract language that warrant a review with our attorney to assure the appropriate contractual protections are in place.

Data Classification

Data classification recognizes that different types of data require different types of securing. For example, public information, such as an individual's name, address, and phone number are, typically, considered to be public information because it is readily available (in the phone book, for example). Because it is public information, the duty of care associated with that data is less than if the individual's social security number, date of birth, drivers' license number, or credit

card account number were included with the previously listed information. In situations where nonpublic information is obtained, it has become more and more important to take additional precautions to secure and protect the data.

GIAC should develop a data classification strategy and policy that helps employees recognize when they are dealing with nonpublic personal information and the steps they should take to secure it. Policies should developed that include the appropriate handling for data transmitted electronically, mailed from the office, faxed out of the office, or stored via paper copy. The same degree of attention should be extended to discussions with co-workers in or out of the office or over the telephone.

Current Events

Few, if any, businesses operate in a vacuum and have the luxury of not paying attention to what is going on in the environment around them. Hot topics, such as outsourcing and the use of Social Security Numbers, frequently gain the attention of legislators and in some cases, can have potential tax implications and/or result in costly compliance efforts. Staying in tune with public policy issues is just as important as staying in tune with information security best practices.

With this in mind, it is suggested that employees be encouraged to increase their awareness of these types of issues. This may be accomplished by posting pertinent information to the company Intranet web site. Information security staff members are also encouraged to keep an eye on technological developments such as new encryption methods and wireless technologies that are developing, as well as enhancements that are being worked on for software that is currently in use at GIAC. Having a well informed work force is important to the long term success of the organization.

Product Considerations

Previous reference has pointed out the suggested inclusion of intrusion detection systems in the proposed security architecture, but did not provide further evaluation. The study implied the use of network intrusion detection systems (NIDS), rather than considering the benefits that may result from using host intrusion detection systems (HIDS) or a combination of the two.

HIDSs evaluate traffic at a more granular level than NIDS allows due to its deployment to individual host workstations or servers. This functionality enhances the ability of a system administrator to identify concerns and possible attacks on an individual component basis, for example. When HIDS and NIDS work together, they identify individual component concerns, as well as network impact concerns, such as simultaneous attacks on multiple machines.

Research has found a product that is a network IDS, but can be configured to provide "focused monitoring" similar to the benefits provided by a host IDS. "Snort" provides cross-platform network security and is a packet sniffer and logger that offers real-time alerting capability. It "decodes the application layer of a packet and can be given rules to collect traffic that has specific data contained within its application layer."[39]

In terms of "focused monitoring," Snort watches "a single node or service on a network for signs of hostile activity. *To achieve this result,* a single Snort sensor would be deployed with a rule set that covers all known attacks for that device and would provide highly focused monitoring of that traffic on the system."[40] For example, rules would be established regarding port 443 to monitor the web purchase server.

Snort is a free utility that has obtained wide spread accepted and has a highly supported rule database. In addition, it is recognized for being easy to implement and maintain.[41] It is recommended that Snort be deployed at GIAC as a NIDS, configured with rules for network evaluation and located at the network points identified in Figure 1. It is further suggested that Snort be used, at least on a temporary basis, as a focused monitor via sensor deployment for each of the DMZ subnet servers, the Intranet database subnet servers, and the Intranet servers subnet servers.

Additional evaluation is recommended to evaluate other HIDS devices that could be utilized. Potential solutions include Tripwire, GFiLANguard S.E.L.M., and INTRUST Event Admin. An initial study may wish to include a review of two articles written by Ricky M. Magalhaes. Both articles are outlined in the Reference section of this document.

The study mentioned in passing the use of Norton anti-virus software, but did not provide any explanation as to the deployment of this tool. It is suggested that further research be conducted to determine if Norton is the best fit for GIAC's needs. Evaluation must be conducted to determine the degree of deployment utilized – i.e. servers only, workstations only, or some combination thereof. In addition to the Norton product, others that may be considered are McAfee VirusScan and eTrust EZ Antivirus 2005.

Total Cost of Ownership

Simply purchasing new computer hardware or software is only the start of costs a company will incur over the projected life time of the equipment. Additional costs also include implementing the solution, training staff members, maintaining the solution, and other miscellaneous costs, such as scaling, disposal of the hardware, and contingency planning. To assist in the evaluation process, a spreadsheet was developed. The spreadsheet provides flexibility to include costs not originally anticipated and allows for adjustment of hourly rates of pay

and the number of employees. While most companies depreciate hardware over five years, and software over three years, the design of the spreadsheet allows the user to alter this time line. However, depreciation is not taken into consideration within this evaluation.

A series of tables follow below to provide the reader with an understanding of the development of the total cost of ownership for the recommendations contained within the study and this document.

Hardware/Software and Service Contracts Price List			
YEAR 1		**Cost/Device**	**Total Cost**
Hardware/Software			
2	Cisco 2621XM Routers	$2,260	$4,520
2	Cisco 3660 Routers	$480	$960
2	Choice Point FireWall-1/VPN-1	$1,800	$3,600
3	Snort NIDS	$0	$0
12	Snort Focused Monitoring	$0	$0
5	Norton Anti-Virus (10 Pack)	$380	$1,900
			$0
			$0
			$0
			$0
	Total Hardware/Software Cost		$10,980
Service Contracts			
	Cisco 2621XM Routers	$660	$1,320
	Cisco 3360 Routers	$660	$1,320
	Choice Point FireWall-1/VPN-1	$299	$598
	Snort NIDS	$100	$100
	Snort Focused Monitoring	$100	$100
	Norton Anti-Virus	$100	$100
			$0
	Total Service Contract Cost		$3,538

Table 1: Hardware/Software and Service Contracts Price List for Year 1.

As indicated by the title, Table 1 provides a summary of the hardware/software investment that would be needed to implement the recommended solution. As in each of the tables, areas shown in yellow represent fields on the spreadsheet that a user may enter data into without disrupting the calculations performed by the spreadsheet.

Estimated Hardware Life	5	Years	**Number**
Estimated Software Life	3	Years	**Employed**
Engineering Hourly Rate	$125		2
IT Analyst/Technician Hourly Rate	$100		4
Project Mgmt Hourly Rate	$150		1
Other (Consultant)	$150		1
Average Employee Hourly Rate	$50		23
(non-engineer, non-IT, non-PM)			

Year 1	**2004**			**Total Cost**
	Estimated Cost	**Estimated Hours**	**Hourly Rate**	
Equipment				
Routers	$5,480			$5,480
FireWalls and VPNs	$1,800			$1,800
NIDS	$0			$0
NIDS (Focused Monitoring)	$0			$0
Norton Anti-Virus	$1,900			$1,900
Combined Annual Maintenance	$3,538			$3,538
Implementation				
Project Planning		40	$150	$6,000
Staff/Consultant Time		15	$150	$2,250
Project Management		60	$150	$9,000
Post-Installation Testing		25	$125	$3,125
Upgrades/Changes	$0	0	$125	$0
Training				
Engineers		70	$125	$17,500
Staff/Consultant Time		2	$50	$2,300
Help Desk		70	$100	$28,000
Training Development		20	$100	$2,000
"Awareness Training" (1 Hr)		30	Varies	$2,100
On-Going Management				
Daily Log Reviews/Auditing		730	$100	$73,000
Periodic Patching		200	$125	$25,000
Configuration Reviews		60	$125	$7,500
Configuration Updates		60	$125	$7,500
Repairs	$5,000	200	$125	$30,000
Supply Replenishment	$2,000	30	$100	$5,000
Other				
Costs to Scale	$0	0	$0	$0
Impact to Future Projects	$0	0	$0	$0
Disposal of Computer Parts	Donation	0	$100	$0
Equipment Removal	Donation	0	$100	$0
Removal of Proprietary Data	$0	0	$100	$0
Contingency Plan	$1,250	30	$125	$5,000
Continuity Plan	$0	30	$125	$3,750
			Year 1 Total	**$241,743**

Table 2: Total Year 1 Cost Calculations

Information from Table 1 is used to populate the “Equipment” portion of Table 2 which provides the estimated cost of implementation, training, monitoring, maintaining, and other costs for Year 1. Again, fields highlighted in yellow within

the spreadsheet may be manipulated by the user. Although not shown here, the spreadsheet also includes comments regarding the estimated hours indicated on the spreadsheet. Separate worksheets were developed within the spreadsheet for each year.

Table 3 which is displayed in Appendix B reflects estimated costs for Year 2. The top portion of the table reflects adjustments made to the estimated hardware and software life, increases in hourly rates for employees, and reflects the addition of add two non-technical employees. Equipment costs were eliminated as it is not expected there will be additional purchases during 2005; however, hours were maintained for service agreements, training, management, and other costs, such as contingency and continuity plan reviews. Similar considerations were made in subsequent years, reflected in Tables 4 through 6, also found in Appendix B.

Combining the bottom line results from each year the recommendations are anticipated to impact, provides a total estimated cost of over $1.1 million dollars (Table 7). This value does not include costs for cables or electricity, nor does it take into account the cost of depreciation. This Total Cost of Ownership will be used to assist in the evaluation of the anticipated Return on Investment for GIAC.

Year	Estimated Annual Cost	Estimated Daily Cost	Estimated Hourly Cost
1	$241,743	$662	$28
2	$180,695	$495	$21
3	$207,676	$569	$24
4	$226,726	$621	$26
5	$246,055	$674	$28
Total	**$1,102,895**	**$604**	**$25**

Table 7: Five Year Total Cost of Ownership Summary

Return on Investment

When evaluating whether or not to implement a project, it is prudent for the company to evaluate its anticipated return on investment (ROI). ROI is defined as "the financial benefit or return received from a given amount of money or capital invested in to a product/service/line of business."[42] In equation form, Return on Investment is shown as follows:

$$\textbf{Return on Investment} = \frac{\textbf{(Gain-Expenditure)}}{\textbf{Expenditure}} \times \textbf{100\%}$$

To assist with this analysis, a separate spreadsheet was developed. This spreadsheet allows the user to alter the number of fortunes sold on a daily basis, as well as the anticipated cost and income for each fortune. An example of this spreadsheet is provided in Table 8.

Income Assumptions: Year 1	US	Other Countries	Daily Total	Days	Total Annual Consumption
Daily Consumption of Fortunes	40,000	20,000	60,000	365	21,900,000
Income per Fortune	$0.02	$0.02			
Cost per Fortune	$0.01	$0.01			
Net Income per Fortune	$0.01	$0.01			$0.01
Net Income per Day	$400	$200	$600		
Number of Days			365		
Total Net Income per Year			$219,000		$219,000
Net Income per Hour			$25		

Table 8: Example Income Calculation for GIAC Enterprises

Using the spreadsheet referenced in Table 8, altering the values used can provide the user with an expected break-even point as well as helping to define the ROI for the project. For example, based on the Total Cost of Ownership calculations previously discussed, implementation of the recommendations made in this document would cost GIAC approximately $25 per hour for five years. Using the ROI spreadsheet, the break-even point, defined as the number of fortunes that would need to be sold to cover the costs incurred to establish the system, would be to sell approximately 60,000 fortunes per day. In this case, the ROI would be zero.

$$\text{Return on Investment} = \frac{(\$25-\$25)}{\$25} \times 100\% = 0$$

Applying this process to other sales volumes allowed Table 9 to be constructed, reflecting the expected returns based on adjusting the hourly fortune sales rate.

Hourly Cost to Implement Recommendations:	$25	
Hourly Fortune Sales	**Net Income Per Hour**	**Return on Investment**
100,000	$42	68%
200,000	$83	232%
300,000	$125	400%
500,000	$208	732%
750,000	$313	1152%
1,000,000	$417	1568%
1,250,000	$521	1984%
1,500,000	$625	2400%
2,000,000	$833	3232%
2,500,000	$1,042	4068%

Table 9: Return on Investment Calculation Results

The cost per fortune and income per fortune fields could also be altered to provide similar evaluations. Please note that the ROI calculations presented above include only those expenditures outlined in the Total Cost of Ownership calculations. They do not include other overhead costs, such as sales force salaries, office rent, or advertising. In addition, it should be pointed out that any time duration could be applied with the appropriate adjustments. An hourly view was taken as this would be the most likely representation of "down time" should an attack occur – i.e. should an attack occur, hopefully, the down time would be limited to hours, rather than days, weeks, months, etc.

Based on the return on investment results, before other expenditures, and the expected fortune sales volume, the application of the recommendations outlined in this document are very much in line with GIAC's profit goals.

Information Security Awareness

Prior to establishing an information security awareness program, it is important to have standards and guidelines in place. While GIAC has an information security policy today, it should be compared to industry best practices to assure we have applied due diligence in its development and maintenance. The ISO 17799 standards provide a well validated, best practice approach for developing an information security policy. ISO 17799 outlines ten elements[43]:

- Security Policy
- System Access Control
- Computer and Operations Management
- System Development and Maintenance
- Physical and Environmental Security
- Compliance
- Personnel Security
- Security Organization
- Asset Classification and Control
- Business Continuity Management

Numerous standards and guidelines could be established under each of these elements. Examples include:

- Non-GIAC Approved Software
- System Scanning
- Separation of Duties
- Role Based or Least Privilege Access Controls
- Patch Management Application
- Logging Reviews
- Alert Escalation Path
- Vendor Assessments

- General Information Sharing
- Use of GIAC Resources for Personal Gain
- Building Access
- Information Security Training Requirements

Standards and guidelines should be communicated in a clear, concise, and readily understandable manner, by information security specialists and non-specialists alike. They should be presented in a format that allows for easy search capabilities. Maintenance of the policy on the GIAC Intranet site is recommended.

As a result of the on-going need to keep our employees thinking about security, an annual information security awareness course is suggested. This course would be developed by our own information security staff and would be provided to all employees via a web-based training course. The course should take no more than an hour to complete. Examples of topics of focus for this year should include:

- Social Engineering Situations
- Role Based or Least Privilege Access
- Data Classification
- Vulnerabilities Assessment
- Strong Passwords
- Remote Access
- Legal Issues
- Anti-Virus Protection
- Internal Incident Reporting
- External Incident Reporting Requirements
- Business Continuity Planning
- Internal Audit Procedures
- Who, What, When, Where, and Why Thought Processes
- Virtual Private Networks

In addition to participating in an internal Information Security Awareness course, information security staff members should be encouraged to pursue industry certifications and to attend conferences that will help them to stay in tune with the latest trends and emerging best practices.

Conclusions

Since its inception, GIAC has placed emphasis on securing the various assets it maintains. The recognition of the importance of information security by the Chief Executive Officer and Board Members is to be commended. Your consideration of this proposal reinforces the on-going commitment you have towards maintaining GIAC's position as a favored business partner for our many customers and suppliers.

While the original study could have expanded its scope in a variety of areas, the approach used and the recommendations made are sound and appropriate for a growing organization such as GIAC. The selection of products and services that are highly reputable, integrate well with each other in the overall security architecture, and offer the opportunity to scale to anticipated levels of growth prior to their sunset date, will further establish GIAC's intent to become a world-wide supplier of fortunes.

Information supplied within this document helps to further promote and serve this purpose. Examples include recommending that a vulnerabilities assessment be conducted, expanding discussions regarding the use of intrusion detection systems, recommending additional system testing, and supporting consideration of utilizing secure electronic transaction protocol.

Additionally, development of the Total Cost of Ownership and Return on Investment calculations give further validity to the benefits anticipated by implementing this firewall and related device solution.

It is the author's recommendation that a vulnerability assessment followed by a vendor assessment be conducted during fourth quarter 2004 and first quarter 2005. Upon review of the findings, it is anticipated that the implementation of the firewalls, routers, virtual private networks, intrusion detection systems, and the anti-virus software would undertaken during second quarter 2005. This will require immediate vulnerability assessment activity followed by arranging contact with the identified vendors. Additionally, the information security staff will need to take steps to prepare to respond to employee questions received via the helpdesk, as well as preparing for the implementation itself.

It is further recommended that studies be conducted to evaluate potential host intrusion detection products, as well as other anti-virus solutions, for consideration of future security updates. Similarly, a review of the GIAC information security policy to assure industry best practices are applied is in order. Upon approval, these studies should be completed by the end of third quarter 2005, with reporting at the first available Board meeting.

Appendix A: OPSEC Vulnerabilities Assessment Discussion

"Critical information" refers to resources others would find value in having. For example, at GIAC, our fortunes would be an example of the critical information we maintain. Also included would be the customer information we collect and maintain, employee information, our security policy, information regarding our system architecture (including hardware and software), router and firewall logs, and any forms of intellectual property that may belong to GIAC.

Threats to GIAC could develop from many things, including internal and external exposures. For example, a disgruntled employee may steal fortunes or sabotage the GIAC system, a vendor could fail to provide patches in a timely manner resulting in web site down time if an attack occurred; an on-site fire or a hurricane could result in damages to the facility that houses the network; or, a system administrator could overlook an alert log, allowing an attack to persist without taking appropriate steps to stop and/or mitigate the impact. These are but a few examples of threats and risks that come to mind. A brainstorming session would help to identify additional threats and risks faced by GIAC.

The next step of the process includes evaluating how the company would respond to each of the identified threats and risks to discover potential gaps or weaknesses that might be exploited. In this stage, vulnerabilities may be found that were not associated with a threat or risk. If this occurs, further discussion should be encouraged to assure due diligence is applied.

Also included with the vulnerability assessment step is the identification of possible solutions. For example, employees could be required to sign an ethics agreement that indicates they will not access or use the company's resources for their own gain, a service level agreement could be added to vendor contract language indicating the time frame in which patches must be provided, a business continuity plan could be developed to establish a course of action following a fire or hurricane, and specific procedures could be put into place to assure the "checker is being checked" (meaning there is an audit process in place to confirm the system administrator is fulfilling his or her responsibility with regards to monitoring alert logs).

It should be noted that the solutions identified include people, processes, and technology. Focusing or adjusting efforts to only one or only two of these will not allow a cost effective, long term solution to be identified and implemented.

The next step is to perform a risk versus benefit analysis for each of the identified vulnerabilities and their respective solutions. In some cases, placing a value on a particular asset can be a challenge, but it is necessary to the process.

In the case of valuing intellectual property, The SANS Institute points out several considerations to keep in mind. This includes keeping a list of the intellectual

property that belongs to the company, along with a valuation of the property (the valuation might be based on the market value of the property, the impact of supply and demand on the property's value, the impact of obsolescence, the cost to replace the property, or the amount of income received from the property. Just as the value of your personal assets should be reviewed regularly, so should the value of your intellectual property. And, consideration should be given to intangible benefits gained by having the intellectual property. For example, the value of owning a franchise, having a trained workforce, developing goodwill, and the having established relationships with customers and suppliers would be included in this category.[44]

From a more tangible aspect, the cost of replacing the building that houses GIAC should be contemplated. Considerations would include rebuilding the office, reconstructing the network, relocating to a temporary facility, loss of income during the rebuilding time, loss of valued employees that are unable to be without a paycheck while the business is getting reestablished or operating at a percentage of its pre-loss capacity. These costs should be compared to the cost of establishing, maintaining, and practicing a business continuity program. Presumably, the cost of establishing a business continuity plan would be far less than being out of business for the period of time necessary to rebuild after a loss, so the risk versus benefit analysis would reflect the value of developing a business continuity plan.

This tracks with the fifth portion of the OPSEC Vulnerability Assessment process - implementing the steps needed to avoid or reduce the likelihood that the threat or risk will impact the company or mitigating the events that do occur. In addition to the example given above, an appropriate countermeasure to an inappropriate response to a logged alert, might be to formalize incident handling guidelines and procedures to assure a consistent and well thought out response and then training the employee to prevent the situation from reoccurring.

And, the final stage of any assessment process should be to continually reevaluate the company. As technologies change, new threats and risks arise and new solutions may be available to combat the dangers. Unless someone is conducting a regular evaluation of GIAC's people, processes and technologies compared to the external environment in which it operates, problems will arise.

Once an internal assessment is completed, there may be value in selecting and hiring a vendor to conduct an external assessment of our system. This would help to confirm the findings of the internal review and may lead to the discovery of other exposures that had not been previously considered.

Appendix B: Total Cost of Ownership Years 2-5 Spreadsheets

Estimated Hardware Life	4	Years	**Number**
Estimated Software Life	2	Years	**Employed**
Engineering Hourly Rate	$131		2
IT Analyst/Technician Hourly Rate	$105		4
Project Mgmt Hourly Rate	$158		1
Other (Consultant)	$158		
Average Employee Hourly Rate	$53		25
(non-engineer, non-IT, non-PM)			

Year 2	**2005**			**Total Cost**
	Estimated Cost	**Estimated Hours**	**Hourly Rate**	
Equipment				
Routers	$0			$0
FireWalls and VPNs	$0			$0
NIDS	$0			$0
NIDS (Focused Monitoring)	$0			$0
Norton Anti-Virus	$0			$0
Combined Annual Maintenance	$4,000			$4,000
Implementation				
Project Planning		0	$158	$0
Staff/Consultant Time		0	$158	$0
Project Management		0	$158	$0
Post-Installation Testing		0	$131	$0
Upgrades/Changes	$0	0	$131	$0
Training				
Engineers		20	$131	$5,240
Staff/Consultant Time		0	$53	$0
Help Desk		20	$105	$8,400
Training Development		20	$105	$2,100
"Awareness Training" (1 Hr)		30	Varies	$2,165
On-Going Management				
Daily Log Reviews/Auditing		730	$105	$76,650
Periodic Patching		200	$131	$26,200
Configuration Reviews		60	$131	$7,860
Configuration Updates		60	$131	$7,860
Repairs	$5,000	200	$131	$31,200
Supply Replenishment	$2,000	30	$105	$5,150
Other				
Costs to Scale	$0	0	$0	$0
Impact to Future Projects	$0	0	$0	$0
Disposal of Computer Parts	Donation	0	$105	$0
Equipment Removal	Donation	0	$105	$0
Removal of Proprietary Data	$0	0	$105	$0
Contingency Plan Review	$1,250	10	$131	$2,560
Continuity Plan Review	$0	10	$131	$1,310
			Year 2 Total	**$180,695**

Table 3: Total Year 2 Cost Calculations

Estimated Hardware Life	3	Years	**Number**
Estimated Software Life	1	Years	**Employed**
Engineering Hourly Rate	$138		2
IT Analyst/Technician Hourly Rate	$111		4
Project Mgmt Hourly Rate	$166		1
Other (Consultant)	$166		1
Average Employee Hourly Rate	$56		25
(non-engineer, non-IT, non-PM)			

Year 3	**2006**			**Total Cost**
	Estimated Cost	**Estimated Hours**	**Hourly Rate**	
Equipment				
Routers	$0			$0
FireWalls and VPNs	$0			$0
NIDS	$0			$0
NIDS (Focused Monitoring)	$0			$0
Norton Anti-Virus	$0			$0
Combined Annual Maintenance	$4,000			$4,000
Implementation				
Project Planning		10	$166	$1,660
Staff/Consultant Time		4	$166	$664
Project Management		15	$166	$2,490
Post-Installation Testing		20	$138	$2,760
Upgrades/Changes	$3,000	50	$138	$9,900
Training				
Engineers		20	$138	$5,520
Staff/Consultant Time		0	$56	$0
Help Desk		20	$111	$8,880
Training Development		20	$111	$2,220
"Awareness Training" (1 Hr)		30	Varies	$2,452
On-Going Management				
Daily Log Reviews/Auditing		730	$111	$81,030
Periodic Patching		200	$138	$27,600
Configuration Reviews		60	$138	$8,280
Configuration Updates		60	$138	$8,280
Repairs	$5,000	200	$138	$32,600
Supply Replenishment	$2,000	30	$111	$5,330
Other				
Costs to Scale	$0	0	$0	$0
Impact to Future Projects	$0	0	$0	$0
Disposal of Computer Parts	Donation	0	$111	$0
Equipment Removal	Donation	0	$111	$0
Removal of Proprietary Data	$0	0	$111	$0
Contingency Plan Review	$1,250	10	$138	$2,630
Continuity Plan Review	$0	10	$138	$1,380
			Year 3 Total	**$207,676**

Table 4: Total Year 3 Cost Calculations

Estimated Hardware Life	2	Years	**Number**
Estimated Software Life	0	Years	**Employed**
Engineering Hourly Rate	$145		2
IT Analyst/Technician Hourly Rate	$117		4
Project Mgmt Hourly Rate	$175		1
Other (Consultant)	$175		1
Average Employee Hourly Rate	$59		27
(non-engineer, non-IT, non-PM)			

Year 4	**2007**			**Total Cost**
	Estimated Cost	**Estimated Hours**	**Hourly Rate**	
Equipment				
Routers	$0			$0
FireWalls and VPNs	$0			$0
NIDS	$0			$0
NIDS (Focused Monitoring)	$0			$0
Norton Anti-Virus	$280			$280
Combined Annual Maintenance	$4,250			$4,250
Implementation				
Project Planning		15	$175	$2,625
Staff/Consultant Time		10	$175	$1,750
Project Management		25	$175	$4,375
Post-Installation Testing		30	$145	$4,350
Upgrades/Changes	$4,000	65	$145	$13,425
Training				
Engineers		20	$145	$5,800
Staff/Consultant Time		0	$59	$0
Help Desk		20	$117	$9,360
Training Development		20	$117	$2,340
"Awareness Training" (1 Hr)		30	Varies	$2,701
On-Going Management				
Daily Log Reviews/Auditing		730	$117	$85,410
Periodic Patching		200	$145	$29,000
Configuration Reviews		60	$145	$8,700
Configuration Updates		60	$145	$8,700
Repairs	$5,000	200	$145	$34,000
Supply Replenishment	$2,000	30	$117	$5,510
Other				
Costs to Scale	$0	0	$0	$0
Impact to Future Projects	$0	0	$0	$0
Disposal of Computer Parts	Donation	0	$117	$0
Equipment Removal	Donation	0	$117	$0
Removal of Proprietary Data	$0	0	$117	$0
Contingency Plan Review	$1,250	10	$145	$2,700
Continuity Plan Review	$0	10	$145	$1,450
			Year 4 Total	**$226,726**

Table 5: Total Year 4 Cost Calculations

Estimated Hardware Life	1	Years	**Number**
Estimated Software Life	0	Years	**Employed**
Engineering Hourly Rate	$153		2
IT Analyst/Technician Hourly Rate	$123		4
Project Mgmt Hourly Rate	$184		1
Other (Consultant)	$184		1
Average Employee Hourly Rate	$62		27
(non-engineer, non-IT, non-PM)			

Year 5	**2008**			**Total Cost**
	Estimated Cost	**Estimated Hours**	**Hourly Rate**	
Equipment				
Routers	$0			$0
FireWalls and VPNs	$0			$0
NIDS	$0			$0
NIDS (Focused Monitoring)	$0			$0
Norton Anti-Virus	$280			$280
Combined Annual Maintenance	$4,250			$4,250
Implementation				
Project Planning		30	$184	$5,520
Staff/Consultant Time		10	$184	$1,840
Project Management		25	$184	$4,600
Post-Installation Testing		30	$153	$4,590
Upgrades/Changes	$4,500	65	$153	$14,445
Training				
Engineers		20	$153	$6,120
Staff/Consultant Time		0	$62	$0
Help Desk		20	$123	$9,840
Training Development		20	$123	$2,460
"Awareness Training" (1 Hr)		30	Varies	$2,840
On-Going Management				
Daily Log Reviews/Auditing		730	$123	$89,790
Periodic Patching		200	$153	$30,600
Configuration Reviews		60	$153	$9,180
Configuration Updates		60	$153	$9,180
Repairs	$5,000	200	$153	$35,600
Supply Replenishment	$2,000	30	$123	$5,690
Other				
Costs to Scale	$0	0	$0	$0
Impact to Future Projects	$0	0	$0	$0
Disposal of Computer Parts	Donation	10	$123	$1,230
Equipment Removal	Donation	10	$123	$1,230
Removal of Proprietary Data	$0	20	$123	$2,460
Contingency Plan Review	$1,250	10	$153	$2,780
Continuity Plan Review	$0	10	$153	$1,530
			Year 5 Total	**$246,055**

Table 6: Total Year 5 Cost Calculations

References

Aboba, B. and Dixon, W. "IPsec-Network Address Translation (NAT) Compatibility Requirements." (March 2004) URL: http://www.ietf.org/rfc/rfc3715.txt

Barnes, Vince. "The Common Sense Defense." URL: http://www.htmlgoodies.com/security/firewalls.html

Boot, Henk. "Lab Reports: Security Event Log Monitor." Windows 2000 Magazine. December 2001: 70-72. URL: http://www.gfi.com/lanselm/labreport_win2kmag_selm.pdf

"The Broadband Router Features Guide: The Firewall and SPI." URL: http://www.homenethelp.com/router-guide/features-firewall.asp

Bull, Jon. "Snort's Place in a Windows 2000 Environment." 15 Apr 2002. URL: http://www.snort.org/docs/snort-win2k.htm

Camp, Ken. "ISAKMP/Oakley White Paper." URL: http://ipadventures.com/docs/IKE.pdf

Castelino, Kenneth. "3DES and Encryption." URL: http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html

"Check Point Application Intelligence." URL: http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf

"Check Point Software: FireWall-1." URL: http://www.checkpoint.com/products/firewall-1/

"Check Point Getting Started Guide: VPN-1/FireWall-1 Tutorial (Chapter 6)." URL: http://www.checkpoint.com/support/technical/documents/docs-5.0/getting_started_ng_sp0.pdf

"Check Point Software Technologies Price List (Version NG with Application Intelligence Rev. Q1.3)." Dtd. 9 August 2004. URL: http://pricelist.checkpoint.com/sections/descriptions.asp

"Check Point Software Technologies Price List (Version NG)." URL: http://pricelist.checkpoint.com/sections/Home_Office.asp

"Cisco 2600 Series Multiservice Platforms." URL: http://www.cisco.com/en/US/products/hw/routers/ps259/index.html

"Cisco 2600 Series Routers." URL:
http://www.epinions.com/content_18929716868

"Cisco 2600 Series Router Prices." URL:
http://www.tribecaexpress.com/cisco_2600_price.htm

"Cisco 2621XM Modular Access Router." URL:
http://www.cdw.com/shop/products/default.aspx?EDC=391248

"Cisco 2621XM Multiservice Router." URL:
http://www.tribecaexpress.com/cisco_2621xm.htm

"Cisco Intrusion Detection System – Data Sheet." URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008017efb3.html

"Cisco Intrusion Detection System – Network Module for Cisco 2600, 3600, and 3700 Routers." URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008017dc22.html

"Cisco Intrusion Detection System – Signature List." URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008014c532.html

"Cisco IOS Firewall Data Sheet." URL:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a0080117962.html

"Cisco IOS Firewall Software Application Overview." URL:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a008010e5c7.html

"Cisco IOS Enterprise Plus/H323 MCM – (v. 12.2(8)T) – complete package."
URL : http://www.cdw.com/shop/products/default.aspx?EDC=487096

"Cisco IOS Service Provider – (v. 12.2(8)T) – complete package." URL:
http://www.cdw.com/shop/products/default.aspx?EDC=501378&printable=1

"Cisco IOS Software Release 12.2(18)SXD." URL:
http://www.cisco.com/en/US/products/ps5942/index.html

"Cisco PIX 500 Series Firewalls – Data Sheet." URL:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a00801daa53.html

"Cisco PIX 500 Series Firewalls - Introduction." URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html

Cohen, Beth. "LDAP 101: Glue Your Network's Pieces Together." August 12 2002. URL: http://networking.earthweb.com/netsp/print.php/1444871

Department of Commerce: National Institute of Standards and Technology. "Announcing Approval of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard." Docket No. 98109262-919-02. RIN 0693-ZA 27. URL: http://csrc.nist.gov/cryptval/des/fr991105.pdf

"Deploying GFI LANguard S.E.L.M.: Design Overview and Deployment Strategies." URL: http://www.gfi.com/whitepapers/deploying-languard-selm.pdf

Dwan, Berni. "LANguard Security Event Log Monitor." SC Magazine March 2002. URL: http://www.gfi.com/lanselm/sc-magazine-reprint-(languard-selm).pdf

"Editor's Top Software." 17 Aug 2004. URL: http://reviews-zdnet.com.com/4521-6520_16-5021410-5.html?tag=txt

"Expert Knowledge Base." URL: http://expertanswercenter.techtarget.com/eac/knowledgebaseAnswer/0,295199,sid63_gci980297,00.html

"FireWall-1." URL: http://www.checkpoint.com/products/downloads/firewall-1_datasheet.pdf

Franklin, Curt. "How Operating Systems Work." URL: http://computer.howstuffworks.com/operating-system.htm/printable

Franklin, Curt. "How Routers Work." URL: http://computer.howstuffworks.com/router.htm/printable

"GFiLANguard: Security Event Log Monitor." URL: http://www.gfi.com/lanselm/lanselmbrochure.pdf

"GFiLANguard: Security Event Log Monitor – Pricing." URL: http://www.gfi.com/pricing/pricelist.aspx?product-LANSELM&print=1

"GFI LANguard Security Event Log Monitor 4." URL: http://www.snapfiles.com/features/eventmonitor-803-418080.php

"The GNU Privacy Guard." URL: http://www.gnupg.org/(en)/index.html

Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf

Honda, Gail and Martin, Kipp. The Essential Guide to Internet Business Technology. New Jersey: Prentice Hall PTR, 2002.

"How to Detect Hackers on Your Web Server." URL: http://www.gfi.com/whitepapers/detect-hackers-on-web-server.pdf

Innella, Paul. "Network Security Design and Implementation." URL: http://www.ph.utexas.edu/security/network-security.html

"Introduction to SSL." URL: http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

"The ISO 17799 Directory." URL: http://www.iso-17799.com/

"ISO 17799 Made Easy." URL: http://www.iso-17799-security-world.co.uk/def.htm

Kalakota, Dr. Ravi and Robinson, Marcia. e-Business 2.0: Roadmap for Success. New Jersey: Addison-Wesley, 2001.

Magalhaes, Ricky M. "Host-Based IDS vs. Network-Based IDS (Part 1)." URL: http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html

Magalhaes, Ricky M. "Host-Based IDS vs. Network-Based IDS (Part 2 – Comparative Analysis)." URL: http://www.windowsecurity.com/articles/Hids_vs_Nids_Part2.html

Orman, H. "The OAKLEY Key Determination Protocol." URL: http://www.ietf.org/rfc/rfc2412.txt (Nov 1998)

"PGP Command Line FAQ." URL: http://www.pgp.com/products/commandline/faqs.html

"PGP Command Line Product Features." URL: http://www.pgp.com/products/commandline/features.html

"PGP Command Line Technical Specifications." URL: http://www.pgp.com/products/commandline/techspecs.html

Pidgeon, Nick. "How Ethernet Works." URL: http://computer.howstuffworks.com/ethernet.htm/printable

"RFC Editor." URL: http://www.rfc-editor.org/

Roesch, Martin. "Snort: Lightweight Intrusion Detection for Networks." URL: http://www.snort.org/docs/lisapaper.txt

SANS Security Leadership Essentials for Managers – Track 12: Defense In-Depth (12.2). SANS Institute, 2004.

SANS Security Leadership Essentials for Managers – Track 12: Internet Security Technologies (12.3). SANS Institute, 2004.

SANS Security Leadership Essentials for Managers – Track 12: Management Practicum (12.5). SANS Institute, 2004.

SANS Security Leadership Essentials for Managers - Track 12: Managing the Plant, Network, and Information Architecture (12.1). SANS Institute, 2004.

SANS Security Leadership Essentials for Managers – Track 12: Secure Communications (12.4). SANS Institute, 2004.

"S/Key." URL: http://www2.kr.freebsd.org/handbook-new/skey.html

"SSL Certificates – Strong Encryption – Strong Warranty." http://www.digicert.com/128-bit-ssl-certificates.htm

Telkamp, Thomas. Update by: Huizer, Erik. "Security: S/Key." URL: http://www.surfnet.nl/innovatie/surf-ace/security/doc/skey.html (Sept 1996)

"10 Tips for Creating a Network Security Policy." URL: http://secinf.net/info/policy/10tips.htm

"Triple-DES (3DES)." URL: http://www.itsecurity.com/dictionary/3des.htm

"Tripwire for Network Devices Data Sheet." URL: http://www.tripwire.com/files/literature/product_info/Tripwire_Network_Devices.pdf

Tuttle, Steven; Ehlenberger, Ami; Gorthi, Ramakrishna; Leiserson, Jay; Macbeth, Richard; Owen, Nathan; Ranahandola, Sunil; Storrs, Michael; and Yang, Chunhui. "Understanding LDAP: Design and Implementation." URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf

Tyson, Jeff. "How Firewalls Work." URL: http://computer.howstuffworks.com/firewall.htm/printable

Tyson, Jeff. "How Network Address Translation Works." URL: http://computer.howstuffworks.com/nat.htm/printable

Tyson, Jeff. "How Virtual Private Networks Work." URL: http://computer.howstuffworks.com/vpn.htm/printable

"Using S/key." URL: http://www.inch.com/info/tech/faqs/skey.html

Various Authors. Editors: Tipton, Harold F. and Krause, Micki. Information Security Management Handbook, 4th Edition. Auerbach Publications, CRC Press LLC, 2000.

Various Authors. Editors: Tipton, Harold F. and Krause, Micki. Information Security Management Handbook, Volume 2, 4th Edition, Vol. 2. Auerbach Publications, CRC Press LLC, 2001.

"VPN-1/FireWall-1 – Performance Brief." URL: http://www.checkpoint.com/products/firewall-1/vpn-1_firewall-1_perfdetails.html

"VPN-1/ FireWall-1/FloodGate-1 – Application Support." URL: http://www.checkpoint.com/products/firewall-1/vpn-1_firewall-1_appsupport.html

"What is LDAP?" URL: http://www.gracion.com/server/whatldap.html

Endnotes

[1] SANS Security Leadership Essentials for Managers – Track 12: Management Practicum (12.5). The SANS Institute, 2004. pp. 14.
[2] SANS Security Leadership Essentials for Managers – Track 12: Defense In-Depth (12.2). The SANS Institute, 2004. Ch. 6, pp. 3, 6-8.
[3] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 5.
[4] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 5.
[5] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp.4.
[6] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 5-6.
[7] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 6-7.
[8] Tuttle, Steven; Ehlenberger, Ami; Gorthi, Ramakrishna; Leiserson, Jay; Macbeth, Richard; Owen, Nathan; Ranahandola, Sunil; Storrs, Michael; and, Yang, Chunhui. "Understanding LDAP: Design and Implementation." URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf pp. 3.
[9] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 11.
[10] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 14.
[11] Koch, Bryan T. Editors: Tipton, Harold F. and Krause, Micki. Information Security Management Handbook, *Enclaves: The Enterprise as an Extranet*. Vol.2, 4th Edition. Auerbach Publications, CRC Press LLC, 2001. pg. 154.
[12] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 15.
[13] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 16.
[14] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 17.
[15] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 17.

[16] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 17.
[17] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 19.
[18] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 19.
[19] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 20.
[20] Blanding, Steven F. Editors: Tipton, Harold F. and Krause, Micki. Information Security Management Handbook, *Secured Connections to External Networks*, 4th Edition. Auerbach Publications, CRC Press LLC, 2000. pp. 65.
[21] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 31.
[22] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 31.
[23] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 36.
[24] "What is LDAP?" URL: http://www.gracion.com/server/whatldap.html
[25] SANS Security Leadership Essentials for Managers - Track 12: Managing the Plant, Network, and Information Architecture (12.1). The SANS Institute, 2004. Ch. 2, pp. 39.
[26] "Cisco 2621XM Modular Access Router." URL: http://www.cdw.com/shop/products/default.aspx?EDC=391248
[27] "FireWall-1." URL: http://www.checkpoint.com/products/downloads/firewall-1_datasheet.pdf
[28] Camp, Ken. "ISAKMP/Oakley White Paper." URL: http://ipadventures.com/docs/IKE.pdf
[29] SANS Security Leadership Essentials for Managers – Track 12: Secure Communications (12.4). The SANS Institute, 2004. Ch. 20 pp. 16-18.
[30] Hlavac, Dan. "GIAC Certified Firewall (GCFW) Practical Assignment (Version 1.9)." 12 May 2003. URL: http://www.giac.org/practical/GCFW/Dan_Hlavac_GCFW.pdf pp. 4.
[31] The "Snowflake Syndrome" refers to the challenges that result from having computers configured in a inconsistent manner. The analogy references the fact that no two snowflakes are alike. If all computers are configured in the same manner, troubleshooting and error handling are simplified. While system configurations are ideally configured in a similar manner, the access requirements of each tele-worker, mobile sales force member, or corporate

employee should be varied based upon the role they play for the organization. SANS Security Leadership Essentials for Managers – Track 12: Managing the Plant, Network, and Information Architecture (12.1). The SANS Institute, 2004. Ch. 6, pp. 19- 20, 33-34.

[32] SANS Security Leadership Essentials for Managers – Track 12: Internet Security Technologies (12.3). The SANS Institute, 2004. Ch. 14, pp. 18.

[33] SANS Security Leadership Essentials for Managers – Track 12: Managing the Plant, Network, and Information Architecture (12.1). The SANS Institute, 2004. Ch. 3, pp. 17.

[34] SANS Security Leadership Essentials for Managers - Track 12: Defense In Depth (12.2). The SANS Institute, 2004. Ch. 12, pp. 34.

[35] "California Civil Code 1798.29." URL: http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=6904402646+0+0+0&WAISaction=retrieve

[36] SANS Security Leadership Essentials for Managers – Track 12: Defense In-Depth (12.2). The SANS Institute, 2004. Ch. 7, pp. 6-7.

[37] SANS Security Leadership Essentials for Managers – Track 12: Secure Communications (12.4). The SANS Institute, 2004. Ch. 24, pp. 6-7.

[38] SANS Security Leadership Essentials for Managers – Track 12: Management Practicum (12.5). The SANS Institute, 2004. pp. 114-140.

[39] Roesch, Martin. "Snort: Lightweight Intrusion Detection for Networks." pp. 1-2. URL: http://www.snort.org/docs/lisapaper.txt

[40] Roesch, Martin. "Snort: Lightweight Intrusion Detection for Networks." pp. 10. URL: http://www.snort.org/docs/lisapaper.txt

[41] Bull, Jon. "Snort's Place in a Windows 2000 Environment." pp. 1. URL: http://www.snort.org/docs/snort-win2k.htm

[42] SANS Security Leadership Essentials for Managers – Track 12: Internet Security Technologies (12.3). The SANS Institute, 2004. Ch. 15, pp. 4.

[43] "The ISO 17799 Directory." URL: http://www.iso-17799.com/

[44] SANS Security Leadership Essentials for Managers - Track 12: Managing the Plant, Network, and Information Architecture (12.1). The SANS Institute, 2004. Ch. 5, pp. 45-49.

Last Updated: July 27th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Oslo Autumn 2017	Oslo, Norway	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
Community SANS Banff MGT512	Banff, AB	Oct 23, 2017 - Oct 27, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Memphis MGT512	Memphis, TN	Nov 06, 2017 - Nov 10, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced