Global Information Assurance Certification Paper

GISO – Practical Assignment

Information Security Officer

Version 1.2 (February 9, 2002)

GIAC Enterprises: Secured Perimeter Access

Prepared by:

Jorge (Bobby) L. Dominguez

SANS Network Security 2002

Washington, DC

January 16, 2003

TABLE OF CONTENTS

ABSTRACT **1**

ASSIGNMENT 1 – DESCRIBE GIAC ENTERPRISES **2**

GIAC ENTERPRISES – ELECTRONIC DATING 2
IT INFRASTRUCTURE 2
Logical Network Diagram *3*
Secured Perimeter Network Architecture *4*
Border 4
Networks 4
FrontNet (DMZ) 5
MidNet 6
BackNet 7
Secured Perimeter Access (SPA) 7
List of Major Components *9*
Border 9
FrontNet 9
MidNet – BackNet 9
BUSINESS OPERATIONS 9
Corporate 10
Human Resources 10
Managers 10
Customer Service 10
Billing 11
Operations 11
Database Administrators 11
Engineering/Quality Assurance 11

ASSIGNMENT 2 – IDENTIFY RISKS **13**

AREAS OF RISK 13
RISK 1 – EMPLOYEES UNWITTINGLY DISCLOSE PRIVATE INFORMATION 13
Overview *13*
Relevance & Consequences *13*
Mitigation *14*
RISK 2 – UNAUTHORIZED ACCESS VIA WEAK AUTHENTICATION 15
Overview *15*
Relevance & Consequences *15*
Mitigation *16*
RISK 3 – LOSS OF SERVICE AVAILABILITY 16
Overview *16*
Relevance & Consequences *17*
Mitigation *18*

ASSIGNMENT 3 – EVALUATE & DEVELOP SECURITY POLICY **19**

EVALUATE SECURITY POLICY 19
Purpose *22*
Background *22*
Scope *22*
Policy Statement *23*
Responsibility *24*

Action *24*
REVISE SECURITY POLICY 24

ASSIGNMENT 4 – DEVELOP SECURITY PROCEDURES 28

GIAC ENTERPRISES LOCKDOWN PROCEDURE 28
Purpose *28*
Scope *28*
Stage-1 Lockdown 28
Stage-2 Lockdown 28
Stage-3 Lockdown 29
Procedure *29*
Responsibility *31*
Human Resources 31
Information Security Manager 31
Security Administrators 31
System Owners 31
Revision History *31*
References *31*

APPENDIX A – SPA MATRIX 32

APPENDIX B – EMPLOYEE ACCESS REQUEST FORM 34

APPENDIX C – LOCKDOWN NOTIFICATION SCHEDULE 35

APPENDIX D – ROUTER ACL PREAMBLE 36

APPENDIX E – SECURE LINUX TEMPLATE RPMS 37

REFERENCES 40

ABSTRACT

The following document, “GIAC Enterprises: Secured Perimeter Access”, contains the 4 assignments defined in the GISO Basic Practical Assignment v1.2 from February 9, 2002. The assignment requires the GISO certification candidate to identify the risks and develop the appropriate security policies and procedures for GIAC Enterprises, a fictional company.

Assignment #1 provides a brief description of GIAC Enterprises, its information technology, infrastructure, and its business operations. These elements are used to identify the risks in Assignment #2. In Assignment #3, the candidate demonstrates his ability to read and evaluate a policy, identifying strengths and weaknesses and making recommendations to improve the policy for one of the risks previously identified. In Assignment #4, the candidate will use the existing policy to develop procedures to implement and enforce the policy.

ASSIGNMENT 1 – DESCRIBE GIAC ENTERPRISES

GIAC Enterprises – Electronic Dating

GIAC Enterprises was the first electronic dating service on the Internet, offering members the ability to search thousands of profiles in order to find a friend, pen-pal, lover or mate. GIAC provides an environment where people can socialize and find the person they are looking for, without leaving their home. Although GIAC collects personal data on its members, all members retain anonymity because real names and addresses are never collected or displayed. Only when a member purchases a subscription electronically (e.g. via credit card), is an "identifying" piece of information required.

Members begin by creating an account and answering multiple-choice questionnaires and free-text essay questions. This is the core of a member's profile. The questions range from basic demographic information, such as "salary range" and "education level", to general interests, such as "favorite outdoor activity" or the member's "expectation on a first date". After the account is created, members can search and filter through thousands of profiles and find those of interest through a variety of tools. At the same time, their profile becomes available for others to search. Communication between members is handled by internal mail servers and never leaves the site unless the member addresses it to an outside e-mail address.

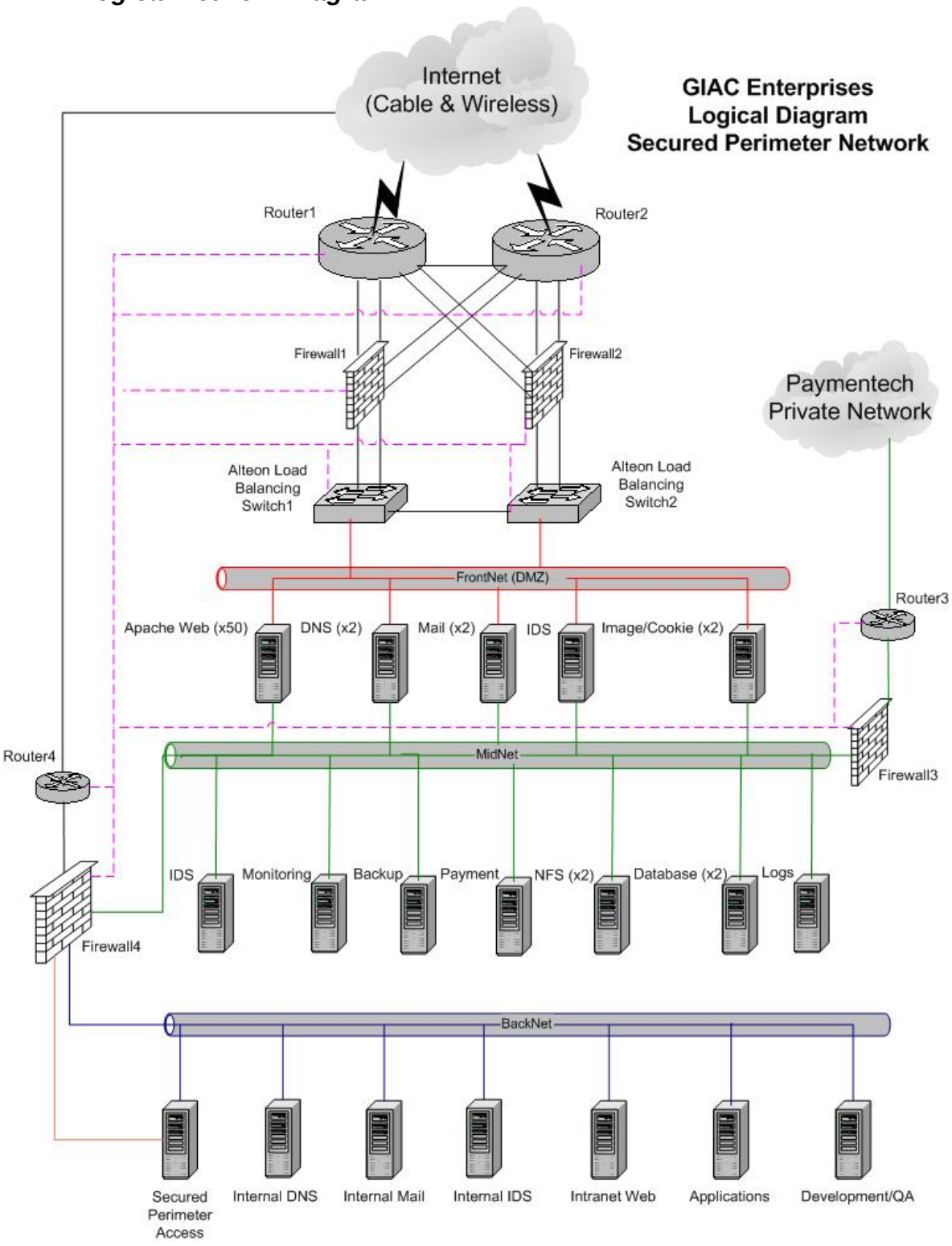
GIAC Enterprises is a subscription-based, online service operating out of a small office that serves as a data center and "headquarters". GIAC's 55 employees, consisting of engineering, operations, customer service, and human resources, typically work from home offices, distributed around the country. This distributed company model for employees adds an additional challenge to securing the infrastructure while providing easy Internet access to customers and employees.

IT Infrastructure

Because GIAC Enterprises' members voluntarily provide personal information for their profiles, privacy and security are critical to the company's business model. Furthermore, the decentralized nature of its management, development and operations requires a secure IT infrastructure. The GIAC Secured Perimeter Network (SPN) is designed to provide high availability and performance to critical services as well as a "defense in depth"[1] strategy.

[1] Fried, p. 1-28

Logical Network Diagram[2]



[2] This diagram describes a "real" network designed and implemented by the author. It has been sanitized to preserve the confidentiality of the company.

Secured Perimeter Network Architecture

Border

All of GIAC's production traffic is routed through 2 Cisco 7507 routers (Routers #1 and #2 in the diagram), running IOS 11.1.28, to Cable and Wireless's Internet peering network. Routers #1 and #2 announce only the FrontNet (DMZ) network using BGP. The routers are cross-connected and configured for load balancing and automated failover. The routers run an earlier, simpler version of IOS that is stripped down of extra protocols for stability and efficiency. All routers contain a basic access control list (ACL) "preamble" to block spoofing and incoming IP's matching those from the GIAC networks. (See Appendix D for a sample ACL.)

Behind the routers are redundant Nokia IP740[3] firewalls (Firewalls #1 and #2 in the diagram), running IPSO 3.5 FCS8 and Checkpoint Firewall-1[4] NG FP2. With hot-swappable components and redundant power supplies, the Nokia IP740 provides maximum uptime as well as almost 2 Gbps firewall throughput. The Nokia firewalls use Virtual Router Redundancy Protocol (VRRP)[5], based on RFC 2338 and 2787, to maintain a high availability environment. The firewalls are configured with basic filters that allow only web, mail and DNS traffic to the FrontNet. The filters further segregate traffic to specific servers. For instance, SMTP traffic is only allowed to the Mail servers, web traffic is restricted to the Web servers, etc… The firewalls also act as a first line of defense against harmful traffic. Only Web, DNS, and mail traffic is allowed into the Production Network:

- Port 80 (www)
- Port 443 (secure WWW)
- Port 25 (sendmail)
- Port 53 (DNS)

The Alteon 184e switches, running Web OS 10.0.25, are used to provide load balancing and failover to the web server farm in the FrontNet. The Alteon's also provide automated failover to the Image, Mail and external DNS servers. If a server fails to respond properly, the Alteon's automatically take it out of service and sets an SNMP trap for monitoring.

Networks

The GIAC IT Infrastructure is divided into 3 networks: FrontNet, MidNet, and BackNet. By utilizing 3 separate networks, GIAC is able to keep unsecured traffic, confidential information, high bandwidth applications, corporate traffic and end-users from interacting. Each network segment is monitored by its own IDS system, running Snort and customized analysis scripts. The FrontNet, MidNet and BackNet ethernet networks use Cisco 2924 switches.

[3] IP Network Security Solutions. http://www.nokia.com/pc_files_wb2/NOK_IP740_DTS.pdf
[4] Check Point Firewall-1 Technical Overview. http://www.checkpoint.com/products/downloads/firewall-1_techbrief.pdf
[5] VRRP, Virtual Router Redundancy Protocol. http://www.networksorcery.com/enp/protocol/vrrp.htm

The FrontNet handles traffic that communicates directly with the public via the Internet. This is the network that end-users use to send e-mail and access the GIAC Dating Service (GDS) Web application. GIAC serves approximately 10 million web pages and 685,000 e-mails per day, using approximately 40 Mb/s in total bandwidth. The network itself can handle considerable growth and was designed with that in mind. By its very nature, the FrontNet is the most exposed segment of the network, particularly to DoS attacks. Making the Border as resilient and redundant as economically possible has mitigated the potential damage from DoS attacks.

The MidNet is used for secure server-to-server communication. It connects the FrontNet servers to the database, log, backup and monitoring servers via a second NIC. Inter-server access is restricted by specific TCP Wrapper entries on both FrontNet and MidNet hosts. Each segment's IDS server monitors the traffic between the FrontNet and MidNet servers. If a FrontNet server is compromised and the TCP Wrappers are changed, the IDS would detect the unexpected connection attempts. Traffic on the MidNet includes NFS, Free Veracity (file integrity checking), internal payment (credit card) servers, backups and system management.

The Backnet is the main corporate network used for the Intranet, internal mail and DNS, development and QA, and internal applications. The SPA server on the BackNet provides the authentication of all employees based on the SPA Matrix.

All network management (diagramed in magenta) is handled via a screened Management Network connected to the VPN serviced by Firewall #4 and the Secured Perimeter Access (SPA) server. An administrator connected to the SPA server can connect to any network device without transmitting traffic via any production network.

FrontNet (DMZ)

The FrontNet (diagramed in red) is the DMZ segment, consisting of 50 Apache web servers, 2 Mail servers, 2 Image servers, 2 external DNS servers and an IDS server.

All GIAC servers run a "hardened" version of RedHat Linux 6.2 running the 2.4.18-3 kernel and a variety of RPM patches. (See Appendix E for a list of the basic RPMs installed.) The only exception to this is the Application server on the BackNet that runs Windows 2000 Professional. The secure "GIAC Linux Template" is created by installing the minimum number of packages required from the basic RedHat distribution and using tools such as "Bastille"[6] to secure the operating system. Each server only runs the services required for its specific function. In keeping with the defense-in-depth strategy, all servers employ multiple security layers:

[6] Bastille Linux. http://www.bastille-linux.org/

- PortSentry is utilized to automatically block any IP accessing a port that is closed or sending TCP/IP packets with invalid flags, effectively blocking anyone attempting a port scan of the server.
- The Linux IP Chains feature is used to block access to ports, services and IP's not specifically authorized or violating any host-based firewall rules. IP Chains act as a backup to the ACLs and firewalls in the event that they are disabled.
- All host services use TCP Wrappers to only allow access to/from authorized hosts and services.
- Free Veracity is used to perform file integrity checks on all GIAC systems. This program is based on the client/server model. Each system runs a Free Veracity daemon that only listens on the MidNet. Every 8 hours the IDS system connects to each system, authenticates with an encrypted password, and compares all files and directories with MD5 checksums specified in a configuration file. Every time Free Veracity performs a test, a report is mailed to the GIAC Operations team with the system name and what file was modified. This assists with tracking configuration changes, verifying that programs and configurations have not changed without approval. The program's configuration has been optimized to reduce false alarms.
- "p0f" is used to passively identify a remote system's operating system based on its initial TCP/IP packet. It is only utilized when needed. This tool allows rapid remote system identification, which is helpful during a network attack and subsequent gathering of information for legal purposes.
- All systems transmit their logs via *syslogd* to the Log server; an intruder who modifies the system's logs will not be able to destroy the record of the compromise on the Log server.

MidNet

MidNet servers include 2 Oracle database servers, 2 NFS servers, a Log server, a Backup server, a Monitoring server, a Payment processing server, and an IDS server. Each server on the FrontNet uses a second NIC to route inter-server communications via the "isolated" MidNet (diagramed in green). The MidNet uses private IP space and 2 firewalls to control the type of traffic allowed. It is the main conduit for servers to exchange data. It also offloads NFS and backup traffic from the primary production networks.

The Payment server on the MidNet communicates with a private network owned by Paymentech[7] via a Cisco PIX 525 Firewall[8], running IOS 6.1(3), and a Cisco 7206 router, running IOS 11.1.28, (Router and Firewall #3 in

[7] See Paymentech-GIAC SLA and Paymentech Technical Specification for security implementation details.
[8] Cisco PIX Firewall Series. http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm

the diagram). Credit card payments are handled via an encrypted VPN and a dedicated connection to Paymentech, the credit card processing vendor.

Backups are performed by a Quadratec's Time Navigator software. The Backup server is attached to a Sun L1000 Tape Library system containing 2 DLT tape drives. Quadratec client software runs on all servers and provides a fast and secure connection to the Backup server. All production server backups are performed via the MidNet, however, nightly backups of the corporate servers are performed via the Backnet connection through Firewall #4. The tape library has a capacity for 30 tapes, approximately one month worth of backups. The GIAC Backup Policy document defines the retention period and tape rotation schedule. There is currently no provision for offsite storage of the data.

BackNet

The MidNet is connected to the BackNet (diagramed in blue) via a Cisco PIX 515E Firewall (Firewall #4 in the diagram), running IOS 6.1(3). This firewall runs a VPN and NAT, keeping all BackNet traffic on private IP's. The BackNet is the corporate network and contains the Internal DNS, Mail, IDS, Development/QA, Application and Intranet Web servers. Since almost all of GIAC's corporate applications are web-based, the Intranet Web servers also function as the primary business application server. The Application server is a Windows 2000 Professional system that runs the accounting package and a small number of non-Linux and non-web-enabled applications. Internet access from within the corporate network is provided via Router and Firewall #4 and isolates corporate traffic from the production network. Router #4 is a Cisco 2691 running IOS 12.1(2)T.

Secured Perimeter Access (SPA)

Also attached to the Backnet is the SPA server, the primary access server used to manage the network and servers and access all non-production services. The SPA server contains two NIC's, one connected directly to the firewall using public IP's (diagramed in orange) and one to the private IP BackNet.

SPA is the only system that allows an OS level login (shell/command line access) from outside the GIAC network. Running a proprietary, centralized authentication product, the SPA server uses a further restricted version of the GIAC Linux Template – only SSH services are available on this server.

Each GIAC Enterprise employee has a personal account on this server. Accounts that are not successfully accessed at least once every 30 days are automatically locked. Each employee's account is identified by his or her first and last name, separated by an underscore (_). Employees access SPA via an encrypted VPN session handled by Firewall #4. Once they have connected to the network via the VPN, they must authenticate with the

SPA server. Authentication is simply a matter of entering the username and password at the SSH session login prompt.

Employees are prompted to change passwords every 60 days. Only complex passwords are permitted: containing a mix of upper and lower case letters; containing at least one numeric digit; and containing at least one non-alphanumeric character. Dictionary passwords are not permitted. Quarterly password audits are performed with the "crack" tool, which attempts to guess passwords by brute force.

Once an employee is authenticated into SPA, they can access whichever servers or internal services defined in their access group. When employees login they are presented with a menu of authorized systems and commands. If the menu detects an abnormal exit, it will close the employee's connection.

The menu uses a complex matrix of user and group access levels, the SPA Matrix. The SPA Matrix – a matrix of access levels, groups, servers and services – defines the actual level of access. Each system's sensitivity is defined within the matrix and access is only provided to those requiring it. Additionally, the SPA Matrix defines which services and applications employee can access. (See Appendix A for a partial sample of the SPA Matrix.)

"root" level access is only provided to management level accounts and is highly restricted. Note that at no time does anyone need to know the actual passwords on each system. The SPA server handles all authentication via a combination of keys, username, application and server name. Actual system passwords are complex and long and are only used when first building a server that is not yet part of the network. These passwords are only known to Operations personnel and are maintained in a locked safe at the data center. The passwords are changed quarterly.

All system logins, logoffs, and executed commands are logged on SPA. SPA also collects data on all SSH connections and executed commands occurring on other GIAC systems. Upon login each system sends to SPA:

- Who logged in;
- From where they logged in;
- Login terminal number and IP;
- Process numbers; and
- A time/date stamp.

This information is used to cross reference login logs with the command line logs. Login logs are displayed in real time on the GIAC Monitoring system. In order to collect this data, all GIAC servers use a modified "bash" shell

that uses the *syslogd* facility to log all typed commands to SPA and the Monitoring server.

List of Major Components

Border

Border Router #1, #2	(2) Cisco 7507	IOS 11.1.28
Firewall #1, #2	(2) Nokia IP740	IPSO 3.5 FCS8 Checkpoint Firewall-1 NG FP2
Switches #1, #2	(2) Alteon 184e	Web OS 10.0.25

FrontNet

Router #3	(1) Cisco 7206	IOS 11.1.28
Firewall #3	(1) Cisco PIX 525	IOS 6.1(3)
Switches	(15) Cisco 2924	IOS 12.0(5)WC3b
IDS Server	(1) Compaq DL360	RedHat Linux 6.2/Snort
Web Servers	(50) Compaq DL360	RedHat Linux 6.2/Apache 1.3.22
DNS Servers	(2) Compaq DL360	RedHat Linux 6.2/BIND 9.2.1
Mail Servers	(2) Compaq DL580	RedHat Linux 6.2/Sendmail 8.11.6
Image Servers	(2) Compaq DL580	RedHat Linux 6.2/Apache 1.3.22

MidNet – BackNet

Router #4	(1) Cisco 2691	IOS 12.1(2)T
Firewall #4	(1) Cisco PIX 515E	IOS 6.1(3)
Switches	(9) Cisco 2924	IOS 12.0(5)WC3b
Database Servers	(2) Compaq DL580	RedHat Linux 6.2/Oracle 8i.1.7
NFS Servers	(2) Compaq DL580	RedHat Linux 6.2
Log Server	(1) Compaq DL580	RedHat Linux 6.2
Backup Server	(1) Compaq DL580	RedHat Linux 6.2, Time Navigator
Sun L1000 Tape Library		
Monitoring Server	(1) Compaq DL580	RedHat Linux 6.2
Application Server	(1) Compaq DL360	Windows 2000 Professional, Svc Pack 3
All Other Servers	(7) Compaq DL360	RedHat Linux 6.2

Business Operations

GIAC customers expect a high level of privacy and reliability. Customers access GIAC's dating service via the Internet, using Web browsers. All customer access is via Routers #1 and #2. Customers pay a monthly access fee and expect the service to be available when they wish to use it. This requires a resilient network and server infrastructure, however, the costs of establishing and maintaining such a network can be high.

GIAC's infrastructure balances the need for security, privacy, and availability with the operational costs. Having a telecommuting workforce greatly reduces corporate infrastructure and the associated overhead. In addition, GIAC customers use the service primarily during evening hours and require an enhanced customer service presence during that time. Employees, like customers, use the Internet to access the office. Whereas customers are looking for fast and reliable

access to the dating services, the employees do not necessarily require the same level of redundancy and performance in their connectivity. Employees require access to the Intranet, corporate e-mail, and corporate servers and applications.

As discussed in more detail in the previous IT Infrastructure section, segmenting the GIAC network into the FrontNet, MidNet and Backnet is one method for separating the corporate business from the customers, while using a complementary infrastructure to achieve reliability and security for all parties.

The key access point to the corporate network is via Router and Firewall #4. An employee working from home would establish a VPN session with Firewall #4 and connect to the SPA server via an SSH session. The SPA server will display a dynamic, text menu that provides access to only the servers, applications and services defined by the employee's access rights in the SPA Matrix. (A web-based menu system is planned for the near future.)

Corporate

Corporate employees are defined as those who require access to the ACCPAC Advantage Series Enterprise Edition accounting applications and other services required to manage GIAC's corporate needs. They do not have access to production servers or services.

Human Resources

These employees are a subset of the corporate employees requiring access to payroll systems and private shared directories. They have access to sensitive employee data and thus have the most secure and restricted access rights. The payroll application itself requires its own set of authentication passwords.

Managers

Though they are restricted to their own group access, they can receive specific access as needed. Managers have access to the Monitoring and Backup servers as well as the Internal Mail, Intranet and Development servers.

Customer Service

Customer Service Representatives (CSR's) are critical to GIAC's business. The primary customer service tool is Kana's CRM application, served from the Intranet Application Server. Kana is used to interact with the customers via e-mail and i-mail, an instant messenger-like tool. CSR's also require access to the Database and Log servers to research customer issues. GIAC does not offer customer phone service, but CSR's will call customers if they have a billing issue or the problem cannot be resolved electronically.

Billing

The billing personnel are CSR's with special access to the Payment server containing the credit card and identifying personal data of the customers. Access to the Payment server is highly restricted since this server is the only place where the customer's identifying data is stored. Billing CSR's access the reports on this server to assist customers with subscription issues. They can also issue refunds or other credit card transactions.

Operations

Network Operations Center (NOC) employees have access to all network devices, servers and services, since they maintain them. However, they cannot actually access the private employee data since the HR manager maintains the payroll application passwords. The NOC manager is responsible for maintaining the SPA Matrix. Ops personnel use a variety of custom scripts and tools to maintain servers and the configuration management environment. Monitoring is preformed by a highly customized version of Big Brother.[9]

Database Administrators

The DBA's are specialized NOC personnel who maintain the database servers and assist CSR's with the retrieval of customer service data. Their primary tool is the Oracle Enterprise Manager. Each DBA has the Oracle Client installed on their workstation. Access to the actual database is controlled by port forwarding through the SPA server and its access Matrix.

Engineering/Quality Assurance

Engineering and QA personnel have the same levels of access to the Development/QA server, but are separated into their own groups because they frequently require specific access to Front End (FE) web servers to research bugs or test fixes. The developers use Perforce, a software configuration management tool to manage their software development. In addition, database developers work with DBA's using the Oracle Enterprise Manager, Oracle Client, and Oracle Designer 2000.

The current SPA Matrix can be easily expanded to address changing corporate roles. Additionally, access maintenance is as simple as adding or removing an employee from a group or specific server/service. Temporary access can be added ad hoc, with access terminating automatically based on an access "timer" variable.

For instance, in the sample SPA Matrix in Appendix A, the "mister_manager" employee has access to the Log server as "root". In this example, access was required for a specific research project and was automatically scheduled to expire after a week. If additional access time is required, the process can be repeated.

[9] Big Brother Features. http://bb4.com/features.html

Appendix B contains a sample form for requesting access. Employees complete these forms and submit them to their managers for approval. Access is typically granted within 2 hours of the initial request, assuming manager approval. All approvals are routed via interoffice e-mail.

Each employee is provided with a company laptop that must be used to access the GIAC network. The laptops are pre-configured with the following:

- Broadband connectivity via AT&T Broadband Internet. Any employee not having access to AT&T can have their laptop reconfigured by GIAC NOC personnel.
- VPN client configured to attach to the GIAC VPN.
- Norton Corporate Edition Anti-Virus and Personal Firewall Software with automated virus updates. All employees attaching to the GIAC network receive new updates to the application or virus signature files.
- Tangram, GIAC's asset management client is installed and responds to automatic queries from the Tangram server running on the Application server. Tangram performs an inventory of the laptop hardware and software, confirming that the laptop meets minimum system requirements for attaching to the GIAC network. Disabled virus protection or un-authorized applications on the company laptop will set alerts on the Monitoring system and access may be suspended until the situation is resolved.
- Secure CRT is used for SSH connectivity as well as port forwarding, if needed.
- Kana client for CSR access to customer mail.
- Oracle Client for access to the database.
- Perforce Client for access to the software code base.
- MS Office with PGP enabled.

ASSIGNMENT 2 – IDENTIFY RISKS

Areas of Risk

GIAC Enterprises' success relies on company's ability to protect its customers' data and present a secure and safe environment for people to meet. Because any bad press resulting from a security breach would be detrimental to the company's ability to generate revenue, the corporate attorneys recommended that GIAC Enterprises' Network Operations team perform a risk assessment. The NOC team based their risk assessment on the NIST Risk Management Guide for Information Technology Systems.[10]

Though numerous risks were identified, the following risks were chosen as the most critical to GIAC's business goals:

1) Employees can unwittingly disclose private information
2) Unauthorized access via weak authentication
3) Loss of service availability

Risk 1 – Employees Unwittingly Disclose Private Information

Overview

An employee who is not aware or does not understand the implications of their actions can unwittingly reveal private company or customer information. Native Intelligence, Inc., a security consulting company, states that, "The best way to achieve a significant and lasting improvement in computer security is not by throwing more technical solutions at the problem -- it's by **raising awareness** and training and educating all computer users in the basics of computer security."[11] When you consider that GIAC employees access the company's network from hotels, airports or their homes, uncontrolled and insecure environments, it is apparent that employees can be the company's largest security liability.

Relevance & Consequences

By its very nature, telecommuting provides the employee with a comfortable and relaxed work environment that fosters a reduced vigilance to potential security threats. An unauthorized person could gain access to an employee's or may see printouts containing private data. An employee who is not aware of these threats may not realize that they are putting GIAC Enterprises at risk. Even a "savvy" employee may put the company at risk if they do not always consider the security implications of their actions.

[10] NIST Special Publications 800 Series. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[11] Rudolph, Native Intelligence. Focused on Security Awareness. http://nativeintelligence.com/awareness/whyaware.asp

If the employee's actions or lack of awareness results in an exposure of private data, the potential for damage is immense – a breach of public trust and potential legal liability. There is no question that the customer demographic database and the positive public perception of GIAC's security and privacy are the company's "crown jewels". Any threat to these "jewels" could be financially devastating to company.

Human nature being what it is, the likelihood of any of these events occurring is relatively high. The level of damage may vary, depending on the security violation. Even a minor exposure of data could have negative consequences if it affects the public's perception of trust.

Mitigation

Developing, implementing and auditing employee participation in a security awareness and training program is a quick and relatively inexpensive solution to mitigate the risk. Employees who complete a security awareness program will be more likely to protect access to their laptops. They would be less likely to leave confidential data lying about if they know the value of that information and how it can be use to damage their company.

An effective security awareness program would:

- Develop targeted training programs for management, administrators, developers, customer service representatives, and other employees.
- Train new employees and make them aware of the company's expectations with regards to security. All new employees need to sign the Employee Access Request Form (Appendix B) acknowledging that they have read and are aware of the company's security policies.
- Make all current employees aware of existing security policies, such as "Acceptable Use Policy", "Password Policy", or "Remote Access Policy". If the policies do not exist, create and implement them.
- Add security policies to the Intranet web site and include an electronic bulletin board forum for employees to post their concerns or questions.
- Implement a variety of tools, such as interactive online classes, pamphlets, banners, posters, games or screen savers to raise the employee's awareness.
- Perform bi-annual refresher and tests for security awareness. Post metrics, such as each department's "security awareness level" on the Intranet. Generate some friendly competition between the departments and reward the most "aware" department.
- Engage the employees in the security process to let them know that they are key to securing the company's data. Remind them that they

have the customer's trust and that it is their responsibility to maintain that trust. The integrity of the company primarily relies on the employees and not solely on the technology it deploys.

- Explain what the financial consequences could be if a breach of the public trust occurs due to a publicized security violation. Explain the "crown jewels" and what the damage would be if they were lost. Distribute metrics related to all security issues to department managers so that they understand the impact of ignorance.
- Have a clearly defined course of action in then event of a suspected security violation and periodically test the procedures.

Such a program can be implemented without a large expense. The use of a consulting company that specializes in such services can be pricey, but much of the information is available on the Internet at no cost. The primary costs would be associated with the software or printed materials you develop.

Risk 2 – Unauthorized Access via Weak Authentication

Overview

Remote access is critical to GIAC by keeping overhead costs low. Though many of the typical risks related to remote access have already been mitigated by the use of a VPN, asset management software, virus protection, personal firewall software, and strict access controls, the entire authentication process relies on the quality of the employee's password. A person with malicious intent could guess or gain access to a remote employee's password and have access to the GIAC network.

Relevance & Consequences

All employees understand that their password is important, but they may not be aware of how easy it is to guess or crack passwords. Some employees may use long and complex passwords that cannot be guessed, but they may need to write the password down to remember it. This could expose the password.

A compromised password would provide access to the GIAC network. GIAC's SPA server may reduce the level of access to specific servers, applications or services; however, it will not prevent a hacker from causing significant harm once inside the network. The hacker could perform a denial of service attack from within the network, could plant Trojans that would expose customer data unbeknownst to anyone, or could conduct corporate espionage and steal the company's intellectual property. A complete service outage or an exposure of customer's private data would

impact adversely on consumer opinion and erode confidence in GIAC's ability to provide a private and anonymous service.

Because cracking or guessing passwords is time consuming, it requires a person with a specific agenda to gain access to GIAC. The likelihood for this is moderate. However, any security plan that relies purely on obscurity lacks the depth necessary to make it effective. If a compromise of this nature were to occur, the risk to the "crown jewels" would be high.

Mitigation

GIAC's existing defense in depth Secured Perimeter Network is a good step to mitigating this risk, but it does nothing to address the issue of unauthorized access via a compromised password. The risk can be reduced by:

- Creating and enforcing a Password Policy.
- Changing the SPA server's password authentication to SecureID authentication, based on a two-factor authentication: something you know (e.g. password or PIN) and something you have (e.g. a key card).[12]

The costs of implementing two-factor authentication can be high, but are commensurate with the ultimate risk. Such a method of authentication would greatly reduce the risk associated with compromised passwords because it would also require a "key" to gain access. This adds yet another level to the defense in depth strategy. Because passwords would still be required to access applications, an enforceable Password Policy would be an inexpensive method to reduce the associated risks.

Risk 3 – Loss of Service Availability

Overview

The primary goal of a denial of service (DoS) attack is to prevent legitimate users of a computer-related service from using that service by denying access to a particular resource, such as a network or server. GIAC Enterprises has taken a significant and costly number of steps to ensure the availability of their network and services. However, denial of service (DoS) attacks have no comprehensive solution – no silver bullet – because attackers can control other, more vulnerable systems and use them against a secure site.

Thus, although GIAC has hardened its own servers to prevent having them used as a part of a distributed attack, currently available technology does

[12] SecureID. http://www.rhyshaden.com/secureid.htm

not prevent GIAC Enterprises from becoming a victim. Without a technological solution, GIAC must consider a risk management solution.

Relevance & Consequences

There are several types of DoS attacks that have varying degrees of impact, depending on the underlying infrastructure:

- Bandwidth/Throughput Attacks: These attacks consume resources such as bandwidth or hardware throughput. As the links fill up, legitimate traffic slows down and timeouts occur, causing retransmission and even more traffic.
- Protocol Attacks: These attacks use the expected behavior of TCP, UDP and ICMP protocols to flood a network with traffic and deny the legitimate flow of normal traffic. These attacks go by such names as SYN flood, Smurf and Fraggle.
- Software Vulnerability Attacks: These attacks exploit vulnerabilities in network software, such as a web server or the underlying TCP/IP stack (e.g. teardrop, land, ping of death, naptha, etc…)

DoS attacks can be destructive because of a combination of effects. For example, an attack that does not fully consume bandwidth or overload equipment throughput may be effective because it generates enough malformed traffic to crash a particular service, such as a web server or mail server. Attacks that consume shared resources, such as upstream bandwidth from an ISP, may affect GIAC Enterprises, even though they were not the target of the attack.

The typical consequences of a DoS attack can range from slow access to complete disconnection from the network. End-users would see a site that is slow or non-responsive and may attribute it to poor service quality. This would negatively affect consumer opinion. In addition, it would prevent subscribers from accessing their accounts. Customers may demand refunds or not renew their membership because of the poor experience. All of these would have a negative impact to short and long term revenues.

There are also hidden costs associated with DoS attacks. GIAC has already bared some of these additional costs because of the need to size resources, such as logs and mail spools, to absorb attack-related events. Network traffic generated by an attack will result in incremental bandwidth costs with Cable & Wireless. And finally, GIAC could be burdened with insurance or legal fees or possible third-party liability resulting from its involvement in an attack.

Mitigation

As previously stated, combating DoS is primarily an exercise in risk management. The following business and technical approaches can provide a multi-pronged approach to mitigating the risk:

- Provide excess capacity to absorb some attacks – add extra bandwidth and router throughput.
- Implement defensive network equipment such as firewalls, load balancing and traffic-shaping technology.
- Distribute web services to avoid a single point of attack with services, such as Akamai or Digital Island, or with redundant ISP's and data centers.
- Purchase insurance to cover the costs of DoS attacks.
- Prepare Cable & Wireless, GIAC's ISP, to respond quickly to attacks – get a 4 hr response guarantee.
- Retain a managed security service to handle attacks.
- Employ experienced security staff that can quickly recognize and react to an attack, since a DoS attack may be indistinguishable from a heavy, but legitimate, load on the network.

Because mitigation strategies for attacks and heavy, legitimate traffic may be similar, the costs associated with planning for such an eventuality can be partially included with general capacity planning.

A Business Continuity Plan should be in place to address the recommendations. GIAC should take steps to ensure that critical services continue in spite of attacks or failures. The increased complexity of the network will mean increased costs but may save GIAC from more serious long-term damages. The Business Continuity Plan should also address the loss of critical and non-critical systems.

And finally, because each attack has its own idiosyncrasies, GIAC should be prepared to deploy customized technical remedies as needed. Incident Handling Procedures should be flexible enough to permit the implementation of quick and non-traditional technical as well as non-technical solutions.

The Cooperative Association for Internet Data Analysis (CAIDA) concludes in their paper, Inferring Internet Denial-of-Service Activity, that "…we have observed widespread DoS attacks in the Internet…"[13] The report indicates that the risk of a DoS attack is very high. The cost of mitigating the risk is also very high, but justified, considering the consequences to GIAC's business.

[13] Moore, Voelker, Savage, p.12.

ASSIGNMENT 3 – EVALUATE & DEVELOP SECURITY POLICY

Evaluate Security Policy

The following Remote Access Policy is from the University of Bristol and can be found on the Web at "http://www.bris.ac.uk/ISC/bs7799/remoteaccesspol.htm"[14]. The policy is a publicly available sample from their BS7799 Pilot Implementation. This policy addresses one of the mitigation techniques discussed in Assignment #2, Risk #1.

Security Policy for Remote Access by Staff

Intent

Remote working is seen as a key part in the Company's strategy to promote flexible working practices. The aim of this remote access security policy is to allow the Company to exploit the business benefits of a secure remote access service and to manage the associated risks effectively. Willful or negligent disregard of this policy should be investigated and may be treated as a disciplinary offence.

Definition

For the purpose of this policy, remote access is defined as: "*The ability, for an organisation's staff, to access corporate information and systems from a remote location, across an external telecommunications service*".

Scope

This policy covers all types of remote access, whether fixed or 'roving' including:

• traveling users (e.g. sales and marketing staff)
• home workers (e.g. IT support, Research and Development staff)
• remote office workers (e.g. maintenance engineers).

Risks

The Company recognises that by providing staff with remote access to information systems, risks are introduced, which may result in serious business impact, for example:

* unavailability of network, systems or target information
* degraded performance of remote connections
* loss or corruption of sensitive data
* breach of confidentiality
* loss of or damage to equipment
* breach of legislation or non-compliance with regulatory or ethical standards.

[14] University of Bristol BS7799 Pilot Project. http://www.bris.ac.uk/ISC/bs7799/remoteaccesspol.htm

Objectives

The objectives of the Company's policy on remote access by staff are:

1. To assist business areas to gain competitive advantage by providing secure and resilient remote access in support of the Company's business strategies.

2. To preserve the integrity, availability and, where appropriate, confidentiality of the Company's information and information systems.

3. To manage the risk of serious financial loss, erosion of market share, loss of client confidence or other serious business impact, which may result from a failure in security.

4. To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the Company is adequately protected under computer misuse legislation.

Principles

In providing remote access to staff, the following high-level principles will be applied:

1. A business manager should be appointed to have overall responsibility for each remote access connection to ensure that the Company's policy and standards are applied.

2. A formal risk analysis process should be conducted for each application to which remote access is granted, to assess risks and identify controls needed to reduce risks to an acceptable level.

3. Remote users should be restricted to the minimum services and functions necessary for the business process.

4. Remote access by staff should be governed by formal agreements. These agreements should:

• define clearly the responsibilities of remote users

• outline a code of conduct to which remote workers should adhere

• require the remote user to comply with any necessary security standards and procedures

• be enforceable through contracts and terms of employment.

5. System owners should confirm whether remote access to their systems will be permitted. System owners or the information security manager may prohibit remote access to certain sensitive systems.

6. The confidentiality and integrity of the Company's information should be protected over remote access connections. The level of protection required will be determined by the assessed risk and in some cases may require cryptography-based solutions.

7. Remote access should only be permitted on written authorisation from the head of a business area or delegated authority.

8. The list of authorised remote access users should be reviewed regularly (at least every six months) to confirm that there is still a valid business requirement.

9. Authorisation for remote access should be removed immediately when the connection is no longer required.

10. Responsibilities for security management and administration of remote access should be assigned clearly and training provided where appropriate.

11. Remote users should only access information systems using hardware and software supplied or approved by the Company. An approved standard configuration of hardware and software should be employed.

12. Each remote access user should be identified and authenticated using a strong authentication mechanism (using a token-based system) before access is allowed.

Responsibilities

* The **Board** will be ultimately responsible for ensuring that remote access by staff is managed securely.

* The **Information Security Steering Group** will formulate policy and standards on remote access, ensure that risks are identified and appropriate controls implemented to reduce those risks.

* **Heads of business areas** will be responsible for providing clear authorisation for all remote access users and the level of access provided.

* **System owners** will be responsible for confirming whether remote access to their systems is permitted.

* **Security administrators** will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels.

* **The Information Security Manager** will provide assistance on implementing controls.

* All **remote access users** will be responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources, notify the Company of security incidents and breaches and return all relevant equipment on termination of the connection.

* **Internal auditors** will be responsible for assessing risks and ensuring that controls are being applied effectively

Approved by:

The *Security Policy for Remote Access by Staff*, hereinafter referred to as the Policy, does not use the recommended structure of Assignment #3, but does contain the basic elements as follows:

Purpose

The purpose, why the policy is being established, is clearly described in the "**Intent**" and "**Definition**" sections of the Policy. It defines the purpose as "*The ability, for an organisation's staff, to access corporate information and systems from a remote location, across an external telecommunications service*". In addition, it ties the policy directly to its business with the sentence, "*The aim of this remote access policy is to allow the Company to exploit the business benefits of a secure remote access service and to manage the associated risks effectively*". The final line of the "**Intent**" section, "*Willful or negligent disregard of this policy should be investigated and may be treated as a disciplinary offense*", addresses the consequences of not applying this policy properly. However, it does not detail the disciplinary consequences, leaving flexibility in handling the specific circumstances through standard HR policies.

The issues or risks that the Policy addresses are well defined in the "**Risks**" section. However, the "crown jewels", as they apply to GIAC Enterprises, should also be mentioned to remove any ambiguity of what exactly is at risk.

Background

This optional component is addressed with the first sentence of the "**Intent**" section, "*Remote working is seen as a key part in the Company's strategy to promote flexible working practices*". This clearly ties the policy to the overall business goals. In addition, the entire "**Objectives**" section of the Policy clearly defines and expands upon the risks and purpose of the policy.

Scope

The extent is adequately covered in the "**Scope**" section of the Policy, defining both who and what is covered by the policy, beginning with the statement, "*This policy covers all types of remote access, whether fixed or roving…*". It follows with a bullet list of the types of users affected by the policy. One modification would be to add a statement indicating who needs to read this policy statement – Who is the target audience of the document? Obviously, the policy applies to the personnel described in the scope, but it also needs to be targeted towards those individuals who need to implement the policy. Another minor change would be to rename the department names to reflect GIAC's organizational structure.

Policy Statement

The guiding principles can be found in the "**Principles**" section of the Policy. The Policy contains statements designed to determine what decisions and actions are expedient within the scope of coverage. Each statement is laid out into easy to read numbered list. In addition, the "**Principles**" section within the Policy contains elements reserved for the Action section of the assignment's suggested structure. However, a glaring omission is the exclusion of statements indicating when these policy items must be implemented or when the departments or individuals must comply.

The most obvious problem with this section is the frequent use of the word "should", rather than the words "must" or "will" to make this a true policy statement rather than just a guidelines document.

Statement #1, "*A business manager should be appointed to…*", does not define who appoints the business manager. Though this may be defined in other corporate documents, the statement could be re-written to reflect who is responsible for that task.

Statement #2 states, "A *formal risk analysis process should be conducted…*", but does not define the frequency that the risk analysis should take place. The recommended frequency for GIAC would be every 6 months, based on the company's growth.

Statement #3 states, "*Remote users should be restricted to the minimum services…*", but does not state how this could be accomplished. Using GIAC as the target company for the policy, the restrictions can be accomplished via the SPA Matrix and the SPA Server.

Statement #4 states, "*Remote access by staff should be governed by formal agreements*", followed by bullets defining the agreement contents. An additional bullet should be added that defines who is responsible for maintaining the agreements – Who ensures that they are signed and in place for each employee?

Statement #6 states, "*…and in some cases may require cryptography-based solution.*" GIAC will employ an encrypted VPN for all remote access.

Statement #9 states, "*Authorisation for remote access should be removed immediately when the connection is no longer required.*" In addition, this statement should address how the Operations personnel determine when that condition exists – Do they use an automated timeout of inactive accounts or do they receive formal notification from Human Resources?

Responsibility

This section describes who is responsible for the policy and all of its individual elements. "*The Information Security Steering Group will formulate policy and standards on remote access*…" The word "formulate" can be better defined by describing the Group's responsibility as "drafting, reviewing, approving or modifying" the policy.

Action

This element is part of the "**Principles**" section of the Policy as discussed in the Policy Statement element of the assignment's suggested structure.

The Policy's final line, "*Approved by*", appears trivial and should contain the CEO's and CIO's signature, title line and date of approval. It is important that the policy have a commitment from the executive management to show that they support and agree with the statements.

Overall, this is a well written policy that leaves you with a clear understanding of the issues it is addressing, what steps should be taken to address the issues, and who should carry them out. Despite the need for better wording and more depth to some of the policy statements, it covers the basic elements required for a security policy.

Revise Security Policy

The following policy is a revision of the sample policy from the previous section. It has been modified to correct its shortcomings as well as address GIAC's needs.

GIAC Enterprises
Remote Access Security Policy

Intent

Remote working is seen as a key part in GIAC Enterprises' strategy to promote flexible-working practices, reduce overhead costs, and provide enhanced customer service. The aim of this remote access security policy is to allow GIAC to exploit the business benefits of a secure remote access service and to manage the associated risks effectively. This policy is designed to minimize the potential exposure to GIAC Enterprises from damages that may result from unauthorized use of GIAC resources. Damages include, but are not limited to, the loss of sensitive or confidential data or intellectual property, damage to public image, and damage to critical GIAC systems. Willful or negligent disregard of this policy will be investigated by the Internal Auditors and may be treated as a disciplinary offence, handled by the appropriate Human Resource policies.

Definition

For the purpose of this policy, remote access is defined as: "*The ability, for an organization's staff, to access corporate information and systems from a remote location, across an external telecommunications service*".

Scope

This policy covers all types of remote access, whether fixed or 'roving' including:

• Traveling users (e.g. sales and marketing staff);
• Home employees (e.g. customer service, IT support, development and QA staff); and
• Remote office workers (e.g. human resources and accounting).

The target audience for this policy includes: all GIAC employees, contractors, vendors, and agents using any method of computer communication to connect to the GIAC network or IT infrastructure; or all personnel responsible for implementing IT security policies.

Risks

GIAC Enterprises recognizes that by providing staff with remote access to information systems, risks are introduced, which may result in serious business impact, for example:

- Unavailability of network, systems or target information;
- Degraded performance of remote connections;
- Loss or corruption of sensitive corporate or customer data (crown jewels);
- Breach of confidentiality and privacy (crown jewels);
- Loss of or damage to corporate equipment; or
- Breach of legislation or non-compliance with regulatory or ethical standards.

Objectives

The objectives of GIAC Enterprises' remote access security policy are:

1. To assist business areas to gain competitive advantage by providing secure and resilient remote access in support of GIAC's business strategies;
2. To preserve the integrity, availability and confidentiality of GIAC's information and information systems;
3. To manage the risk of serious financial loss, erosion of market share, loss of customer confidence or other serious business impact, which may result from a failure in security;
4. To comply with all relevant regulatory and legislative requirements (including data protection and privacy laws) and to ensure that GIAC is adequately protected under computer misuse legislation.

Principles

In providing remote access to staff, the following high-level principles will be applied no later than two weeks after the effective date of this policy:

1. System owners will be appointed by the department managers to have overall responsibility for each remote access connection to ensure that GIAC's policy and standards are applied.
2. The internal auditors will conduct a formal risk analysis process for each server, service and application to which remote access is granted. The analysis will assess risks and identify controls needed to reduce risks to an acceptable level. The analysis must recur every 6 months.
3. The principle of least privilege will be applied. Remote users must be restricted to the minimum services and functions necessary for the business process. The SPA Server and Matrix will be the tools used to implement such restrictions.
4. Remote access by staff will be governed by formal agreements, such as the Employee Access Control Form. These agreements should:

   • Clearly define the responsibilities of remote users;
   • Outline a code of conduct to which remote workers should adhere;
   • Require remote users to comply with all security standards and procedures;
   • Be enforceable through contracts and terms of employment; and
   • Be maintained on file for each remote user by Human Resources.
5. System owners will confirm by formal e-mail to Department Managers, HR, Security Administrators and the Information Security Manager whether remote access to their systems, services or applications will be permitted. System owners or the Information Security Manager may prohibit remote access to certain sensitive systems.
6. The confidentiality and integrity of GIAC's information must be protected over remote access connections. The level of protection required will be determined by the assessed risk and will require cryptography-based solutions.
7. Remote access will only be permitted on written authorization (Employee Access Control form) from the Department Manager or delegated authority and Information Security Manager.
8. The list of authorized remote access users will be reviewed quarterly (at least every 3 months) to confirm that there is still a valid business requirement.
9. Authorization for remote access will be automatically removed from any inactive accounts every 30 days. Security Administrators will remove access immediately when the connection is no longer required.
10. Responsibilities for security management and administration of remote access must be assigned clearly and security awareness training must be provided to all employees.
11. Remote users must only access information systems using hardware and software supplied or approved by GIAC Network Operations. An approved, secure standard configuration of hardware and software will be employed.
12. Each remote access user must be identified and authenticated using a strong authentication mechanism (using a smartcard-based system) before access is allowed.

Responsibilities

- The **Board** will be ultimately responsible for ensuring that remote access by staff is managed securely.
- The **Information Security Steering Group** will draft, review, approve and modify policy and standards on remote access, ensure that risks are identified and appropriate controls implemented to reduce those risks. They will be responsible for reviewing the policy at least once per year.

- **Department Managers** will be responsible for providing clear authorization for all remote access users and the level of access provided using the SPA Matrix.
- **Human Resources** will be responsible for handling any disciplinary action as a result of non-compliance with this policy. They will also be responsible for making this policy available via the Security Awareness Program and ensuring that the appropriate access and acknowledgement forms are signed and on file.
- **System Owners** will be responsible for confirming whether remote access to their systems is permitted.
- **Security Administrators** will ensure that user profiles and logical access controls are implemented in accordance with the approved access levels in the SPA Matrix.
- The **Information Security Manager** will provide assistance on implementing controls.
- All **Remote Access Users** will be responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources, notify GIAC Enterprises of security incidents and breaches and return all relevant equipment on termination of their remote access authorization.
- **Internal auditors** will be responsible for assessing risks and ensuring that controls are being applied effectively.

Authorization

Chief Executive Officer: _____

Chief Information Officer: _____

Effective Date: _____
Revision: _____
Revision Date: _____

ASSIGNMENT 4 – DEVELOP SECURITY PROCEDURES

The policy discussed in Assignment #3 requires a variety of procedural documents to implement. However, for the purpose of this assignment only one procedure, that provides detail on how to put the high-level guidance discussed in the policy into effect, will be produced.

GIAC Enterprises Lockdown Procedure[15]

Purpose

This procedure defines the steps necessary for removing access to personnel who no longer require access to the GIAC IT infrastructure, e.g. personnel who are no longer employed by GIAC, in accordance with the GIAC Remote Access Policy. This process is called a "lock down" because, if fully implemented, it will reset all access to the GIAC network, locking out all users using old keys or passwords. The procedure involves the coordinated change of all access controls, passwords and keys, on all devices and applications.

Scope

These procedures apply to all GIAC IT devices, including servers, routers, switches, firewalls, and applications. They are to be implemented upon a triggering event, such as when personnel leave the company. The overall procedure is broken into 3 stages. Each stage defines the scope of the lock down, depending on the triggering event.

Stage-1 Lockdown

This stage is the highest lock down level, requiring changes to all servers, routers, switches, firewalls and applications and is required when key personnel, such as executive managers leave the company. The more access the individual had, the more passwords and keys need to be changed. In addition, a Stage-1 Lockdown is initiated every 6 months in concurrence with the internal audits defined in the GIAC Remote Access Policy.

Stage-2 Lockdown

This is a moderate lock down that primarily involves the support servers and services, but does not include network devices. It is required when NOC personnel leave the company; In other words, anyone having access to the backend IT infrastructure.

[15] This procedure is a copy implemented by the author for his company. It has been sanitized to preserve the confidentiality of the company.

Stage-3 Lockdown

This is a low level lock down requiring changes to only the passwords or keys accessible by the individual who is leaving. It primarily involves application password changes.

Note that because GIAC uses a centralized access server, the most basic lockdown only occurs at this server. Typically locking an employee's account at the SPA server can lock them out of the company's network. This is the most basic implementation of a Stage-3 lockdown.

Procedure

Print the following Lockdown Checklist and follow each step, beginning at the appropriate Stage level as directed by the Information Security Manager. The person completing the work must initial each line item. The document itself must be signed by the NOC and Information Security Managers when complete, to certify that all systems and applications have been secured.

	Admin Assigned	Task
		STAGE-3
❑		Run "Enable Lockdown Stage-3" from the SPA Admin menu to disable Big Brother alerts for 1 hour and notify NOC of password change commencing. This step prevents the monitoring system from triggering false alarms when password files and keys change.
❑		Disable VPN account. This disables access into network so that no one is connected while changes are taking place. This ensures that keys can be reset properly.
❑		Update SPA Matrix. This disables employee's SPA Server account and access to applications and services.
❑		Update master password list on NOCINFO$ share and have new application/server/service passwords approved by the Operations Manager. This ensures that the documentation is updated properly.
❑		Change application passwords, as needed – See System Owners. Some applications use their own authentication methods. These need to be changed if the employee had access to the application.
❑		Change marketing and demo account passwords (Demo123) to production application. See attached Lockdown Notification Schedule.[16] These accounts provide free access to the service and are reserved for Marketing use. The passwords should be changed so that former employees do not access the service.
❑		Notify appropriate Application Managers of new passwords. See attached Lockdown Notification Schedule.
❑		Remove user account from Application, Internal Mail, Intranet, and Development/QA servers, as needed. Remove sandboxes on Development servers, if any. This ensures that the user's accounts cannot be reactivated.
❑		Modify aliases file on Internal Mail server as needed. This prevents mail to continue to route for the employee. In some cases the alias will forward the employee's manager, as needed.
❑		Remove user account from facilities key card system. This prevents access to the data center and offices.
❑		Confirm receipt of all loaned hardware (laptop, monitors, printers, etc…) by HR. Collect company assets
❑		Re-assign all tickets in personnel's box in PTR system to their direct manager. Ensures that work in progress gets rerouted.
❑		Confirm that all user logs on SPA server are backed up and then delete account and directory. This is for historical purposes, in the event that the data is ever required or some former activity needs to be investigated.

[16] A brief and greatly reduced sample of the "Lockdown Notification Schedule" is provided in Appendix C.

❑		Attempt to access and confirm access is denied. Confirm that the changes you have made really were made and work!

STAGE-2

❑		Perform all steps in STAGE-3.
❑		Change GDS general access account on SPA server and propagate with "pwchange" script. The account is the default login from the SPA server. Though no one has access to this password, it is important that it is changes to ensure that the account is not misused. The "pwchange" script propagates the password changes and makes the proper backups and log entries.
❑		Lock "tina" (Backup system) account on SPA server with command "usermod –L tina". Change password and propagate with "pwchange" script. This is the backup system account used by the backup client to connect to servers. The account needs to be locked out to prevent a backup login during the change process.
❑		Change "oracle" account on SPA server and propagate with "pwchange" script. This is the Oracle user account.
❑		Change Oracle database passwords on Database server for users: sys, system, stats, devel. Update Oracle script configuration files containing password hashes. These are the passwords used to access the database itself.
❑		Change "root" account on SPA server and propagate with "pwchange" script. Though no one logs into the "root" account, the passwords need to be changed on SPA and propagated.
❑		Change Big Brother and MRTG passwords on Monitoring server. Ensures that former employees can not get access to monitoring services.
❑		Change .htaccess passwords on Monitoring server for BB, STATS, LOGS, MRTG, SYSMAN, and NOC pages. Ensures that former employees can not get access to the monitoring data.
❑		Regenerate all SSH keys and restart SSH daemons – run "ado mv /etc/ssh/ssh_hosts* /tmp; /sbin/service sshd start", then run "ado /sbin/service sshd restart" to reload the key files. Regenerating the keys ensures that no one can gain access to a server through formerly approved keys.
❑		Make sure that there are no known_hosts in /home/gds/home/.ssh.
❑		Run "update-knownhosts" from Development/QA server.
❑		Force all SPA users to change passwords upon next login. Ensures that a former employee does not have access to another employee's password.
❑		Reboot SPA server. Ensures that all accounts are forced to re-authenticate.

STAGE-1

❑		Perform all steps in STAGE-3 and STAGE-2.
❑		Change Router #1 and #2 passwords.
❑		Change Firewall #1 and #2 passwords.
❑		Change Alteon #1 and #2 passwords.
❑		Change Router #3 passwords.
❑		Change Firewall #3 passwords.
❑		Change Router #4 passwords.
❑		Change Firewall #4 passwords.
❑		Change all switch passwords.
❑		Change SNMP community strings on all devices with "snmp_comm._change" script. Prevents former employee gaining access to SNMP data.

_____ _____

Operations Manager's Signature Information Security Manager's Signature

_____

Date Completed

Responsibility

Human Resources

The HR department informs all department managers of the change in status for any personnel via an e-mail form. This is typically the triggering event for a lockdown. The timing of this event is critical to an orderly lockdown. HR must announce the change prior to or as soon as the staff member knows of the change of status.

Information Security Manager

Based on the HR notification form letter, the manager determines which lockdown stage is required. The manager then informs the system owners and security administrators of the impending lockdown within 1 hour of notification by HR.

Security Administrators

They begin the lockdown as soon as the Information Security Manager informs them. Because a typical lockdown can require a full workday to accomplish, the work preempts any other tasks and includes the entire NOC staff.

System Owners

The individual staff responsible for each system's function will be responsible for completing the changes to passwords for applications on their systems. This is done concurrently with the assistance of the Security Administrators and NOC.

Revision History

Date	Initials	Comments
12/31/02	BBD	Initial draft of procedure
1/15/03	BBD	Added comments to each procedural step

References

GIAC Enterprises Remote Access Security Policy

Lockdown Notification Schedule

SPA Matrix Document

Master Password List (NOCINFO$)

Human Resources Organizational Matrix

Appendix A – SPA Matrix

Employee to Group Matrix

Last Update: Dec-02	dba	billing	ops	qa	eng	mgr	cust srv	corp	hr	special access
joe_employee	X			X	X		X	X		
jane_employee							X	X		
fred_theman		X						X	X	
sos_therope			X					X		
bec_jeff	X			X	X			X		
mister_manager						X		X		Log(root)
chief_head						X		X		

System to Group Matrix

Last Update: Dec-02	dba	billing	ops	qa	eng	mgr	cust srv	corp	hr
Border1			X						
Border2			X						
Firewall1			X						
Firewall2			X						
Firewall3			X						
Firewall4			X						
Alteon1			X						
Alteon2			X						
DNS1-External			X						
DNS2-External			X						
IDS-DMZ			X						
IDS-FrontNet			X						
IDS-BackNet			X						
Image1			X						
Image2			X						
Mail1			X						
Mail2			X						
Monitoring			X			X			
Backup			X			X			
Log			X						
NFS1			X						
NFS2			X						
Payment		X	X						
Database1	X	X	X				X		
Database2	X	X	X				X		
DNS-Internal			X						
Mail-Internal	X	X	X	X	X	X	X	X	X
Intranet	X	X	X	X	X	X	X	X	X
Development	X		X	X	X	X			
Web1			X						
Switch1			X						

Employee to Services Matrix

Last Update: Dec-02	DB Apps	Portal	BB	Perforce	GDS	Kana	ACCPAC	Sol
joe_employee	X			X	X	X		
jane_employee					X	X		
fred_theman		X					X	X
sos_therope			X					
bec_jeff	X			X	X			
mister_manager								X
chief_head							X	X

Appendix B – Employee Access Request Form

EMPLOYEE ACCESS CONTROL FORM

Name:_____ Supervisor:_____
E-mail:_____ E-mail:_____
Phone #:_____ Phone #:_____
Date:_____ Date of Hire:_____

FOR REQUIRED ACCESS:
PLEASE FILL OUT THE TABLE ON THIS PAGE WITH REQUIRED ACCESS INFORMATION.
USE A SEPARATE SHEET FOR ADDITIONAL ACCESS REQUIREMENTS.

Server/Service/Application	Access Method (SSH, Web, Other)	Access Type (User, Admin)

By signing this I agree to abide by the GIAC Remote Access Policy, Acceptable Use Policy, and Password Policy. Additionally, I will not misuse my privileges. I will not share my account with anyone. I will not use anyone else's account to extend my privileges. I will not create new accounts for anyone else.

Signature:_____ Date:_____

Supervisor Signature:_____ Date:_____

Security Authorization:_____Date:_____

The GIAC Network Operations team will evaluate your request. Once we have reached our decision you will be notified as to whether or not your request was approved.

Appendix C – Lockdown Notification Schedule

Name	Phone Number	GDS Photo	GDS Demo123	STATS Web FE	Big Brother	"docs"
Jim Aguya	555-123.4567		X			
Matt Afuller	555-124.5678			x		
Jane Marteliza	555-125.6789	x	x			
Dan Panasevich	555-126.7890	x	x			x
Sally Nocgirl	555-127-8901				x	

Appendix D – Router ACL Preamble

```
!anti-spoofing filter
access-list 100 deny ip <cluster frontnet netblock> any
access-list 100 deny ip <cluster pseudo-frontnet netblock> any
!bogon filter (as defined in RFC3330)[17]
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 169.254.0.0 0.0.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.0.2.0 0.0.0.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 198.18.0.0 0.1.255.255 any
access-list 100 deny ip 224.0.0.0 31.255.255.255 any
!allow tcp sessions sourced from inside our network
access-list 100 permit tcp any any established
!allow ip originating from network mgmt systems
access-list 100 permit ip host 10.10.10.99 any
access-list 100 permit ip host 10.10.10.100 any
access-list 100 permit ip host 222.222.222.48 any
!
!insert proper documented site-specific acl statements here
!all traffic is denied unless specifically allowed
!
```


[17] RFC 3330: Special-Use IPv4 Addresses. http://www.armware.dk/RFC/rfc/rfc3330.html

Appendix E – Secure Linux Template RPMs

anacron-2.1-6
apmd-3.0final-2
at-3.1.8-22.2
authconfig-3.0.3-1
automake-1.4-6
bash-2.05-8.1
bdflush-1.5-11
bind-utils-9.2.1
bison-1.28-2
bzip2-0.9.5d-2
cmafdtn-5.00-1
cmastor-5.00-1
compat-binutils-5.2-2.9.1.0.23.1
compat-egcs-c++-5.2-1.0.3a.1
compat-libs-5.2-2
cpio-2.4.2-16
cpqhealth-1.2.0-1
cvs-1.11.1p1-6.2
db3-utils-3.1.17-4.6x
diffutils-2.7-22.6x
dump-0.4b19-5.6x.1
ed-0.2-19.6x
egcs-c++-1.1.2-30
esound-0.2.20-0
file-3.28-2
fileutils-4.0-21
finger-0.16-5
fnlib-0.4-10
fortune-mod-1.0-11
freetype-devel-1.3.1-5
fwhois-1.00-12
gd-1.3-6
gdbm-1.8.0-3
glib10-1.0.6-6
glibc-2.1.3-23
glibc-profile-2.1.3-23
gmp-2.0.2-13
gpm-1.19.3-0.6.x
groff-1.15-8
gtk+10-1.0.6-6
gtk+-devel-1.2.6-7
gzip-1.2.4a-2
idled-1.16-6
ImageMagick-devel-5.3.3-2
imlib-1.9.13-2.6.x
inetd-0.16-7
initscripts-5.00-1
iplog-2.2.0-2
apache-1.3.22
ash-0.2-20
audiofile-0.1.9-3
autoconf-2.13-5
basesystem-6.0-4
bc-1.05a-5
bigbrother-1.8c-h.2
binutils-2.9.5.0.22-6
byacc-1.9-12
chkconfig-1.1.2-1
cmanic-5.00-1
cmasvr-5.00-1
compat-egcs-5.2-1.0.3a.1
compat-glibc-5.2-2.0.7.2
console-tools-19990829-10
cpp-1.1.2-30
crontabs-1.7-7
db3-3.1.17-4.6x
dev-2.7.18-3
dot-1.0.0-1
e2fsprogs-1.23-2
egcs-1.1.2-30
eject-2.0.2-4
expect-5.28-35
filesystem-1.3.5-1
findutils-4.1-34
flex-2.5.4a-9
fnlib-devel-0.4-10
freetype-1.3.1-5
ftp-0.16-3
gawk-3.0.4-2
gdb-4.18-11
getty_ps-2.0.7j-9
glib-1.2.6-3
glibc-devel-2.1.3-23
glib-devel-1.2.6-3
gnupg-1.0.6-0.6.x
grep-2.4-3
groff-perl-1.15-8
gtk+-1.2.6-7
gtk-engines-0.10-3
hdparm-3.6-4
ImageMagick-5.3.3-2
imap-2000c-1.6.1
indexhtml-6.2-1
info-4.0-5
ipchains-1.3.9-5
iputils-20001010-1.6x

isapnptools-1.21b-1
kbdconfig-1.9.2.4-1
kernel-headers-2.4.18-3
krb5-configs-1.1.1-28
ldconfig-1.9.5-16
less-346-2
libelf-0.6.4-4
libghttp-devel-1.0.4-1
libgr-devel-2.0.13-23
libgtop-1.0.6-1
libjpeg-6b-10
libpng-1.0.5-3
libPropList-0.9.1-1
libtermcap-2.0.8-20
libtiff-3.5.5-2
libtool-1.3.4-3
libungif-devel-4.1.0-4
libxml-devel-1.8.6-2
logd-1.0.0-5
logtail-1.0.0-1
lrzsz-0.12.20-4
ltrace-0.3.10-2
mailcap-2.0.6-1
make-3.78.1-4
man-1.5i2-0.6x.5
mc-4.5.42-10
minicom-1.83.1-1.0.6x
mkinitrd-2.4.1-2
modutils-2.3.21-0.6.2
mouseconfig-4.4-1
ncftp-3.0beta21-4
ncurses3-1.9.9e-11
ncurses-devel-5.0-12
newt-0.50.8-2
ntsysv-1.1.2-1
openssh-clients-3.0.2p1-2
openssl-0.9.5a-4
ORBit-0.5.0-3
passwd-0.64.1-1
pax-1.5-37288
pdksh-5.2.14-2
pidentd-3.0.10-5
portmap-4.0-19
procinfo-17-4
procps-2.0.6-5
psmisc-19-2
pwdb-0.61-0
python-devel-1.5.2-13
qt-2.1.0-4.beta1
quota-2.00pre3-2
rcs-5.7-11
ispell-3.1.20-27
kernel-2.4.18-3
kernel-utils-2.4.18-3
krb5-libs-1.1.1-28
ld.so-1.9.5-13
libc-5.3.12-31
libghttp-1.0.4-1
libgr-2.0.13-23
libgr-progs-2.0.13-23
libgtop-devel-1.0.6-1
libjpeg-devel-6b-10
libpng-devel-1.0.5-3
libstdc++-2.9.0-30
libtermcap-devel-2.0.8-20
libtiff-devel-3.5.5-2
libungif-4.1.0-4
libxml-1.8.6-2
lilo-21.4.4-14
logrotate-3.5.2-0.6
losetup-2.10r-0.6.x
lsof-4.47-2
m4-1.4-12
mailx-8.1.1-16
MAKEDEV-2.5.2-1
man-pages-1.28-6
mingetty-0.9.4-11
mkbootdisk-1.2.5-3
mktemp-1.5-2.1.6x
mount-2.10r-0.6.x
mt-st-0.5b-7
ncompress-4.2.4-15
ncurses-5.0-12
net-tools-1.54-4
nfs-utils-0.3.1-0.6.x.1
openssh-3.0.2p1-2
openssh-server-3.0.2p1-2
openssl-misc-0.9.5a-4
pam-0.72-20.6.x
patch-2.5-10
pciutils-2.1.5-2
perl-5.00503-12
popt-1.6.2-6x
portsentry-1.0-7.3
procmail-3.21-0.62
psacct-6.3.2-1
pump-0.7.8-1
python-1.5.2-27.6.x
pythonlib-1.23-1
qt-devel-2.1.0-4.beta1
raidtools-0.90-6
rdate-1.0-1

readline-2.2.1-6
redhat-logos-1.1.0-2
rmt-0.4b19-5.6x.1
rpm-4.0.2-6x
sash-3.4-2
sendmail-8.11.6-1.6.y
setserial-2.15-3
setuptool-1.2-5
sharutils-4.2.1-2
slang-1.2.2-5
stat-1.5-12
sudo-1.6.4-0.6x.2
sysklogd-1.3.31-17
sysstat-2.1-1
tangram-3.1-2
tcl-8.0.5-35
tcp_wrappers-7.6-10
telnet-0.17.6x-18
termcap-10.2.7-9
time-1.7-9
tk-8.0.5-35
traceroute-1.4a5-24.6x
ucd-snmp-4.2.3-1.6.x.4
unzip-5.40-2
util-linux-2.10f-7
vim-minimal-5.7-0.6x
which-2.9-2
XFree86-devel-3.3.6-29
xntp3-5.93-15
zip-2.3-4
zlib-devel-1.1.3-25.6

readline-devel-2.2.1-6
redhat-release-6.2-1
rootfiles-5.2-5
rpm-devel-4.0.2-6x
sed-3.02-6
sendmail-cf-8.11.6-1.6.y
setup-2.1.8-1
shadow-utils-19990827-10
sh-utils-2.0-5
slocate-2.4-0.6.x
strace-4.2-1
svgalib-1.4.1-2
sysreport-1.0-3.2
SysVinit-2.78-5
tar-1.13.17-3
tcpdump-3.6.2-6
tcsh-6.10-0.6.x
telnet-server-0.17.6x-18
textutils-0.000002
timeconfig-3.0.3-2
tmpwatch-2.8-0.6.x
tree-1.2-7
ucd-snmp-utils-4.2.3-1.6.x.4
utempter-0.5.2-2
vim-common-5.7-0.6x
vixie-cron-3.0.1-40.1
words-37299
XFree86-libs-3.3.6-29
xpm-3.4k-2
zlib-1.1.3-25.6

References

(1) Fried, Stephen. SANS Security Leadership, Part 1: Terms and Concepts. Washington: The SANS Institute, 2002. 1-28.
(2) Dominguez, Jorge. Internal Corporate Network Diagram. Nashua, NH., (Feb. 2000).
(3) Nokia, Inc. (2002). IP Network Security Solutions. *Nokia Corporate Web Site*. http://www.nokia.com/pc_files_wb2/NOK_IP740_DTS.pdf (Dec. 9, 2002).
(4) Check Point Software Technologies, Inc. (Oct. 2000). Check Point Firewall-1 Technical Overview. *Check Point Corporate Web Site*. http://www.checkpoint.com/products/downloads/firewall-1_techbrief.pdf (Dec. 9, 2002).
(5) Network Sorcery, Inc. (2002). VRRP, Virtual Router Redundancy Protocol. *Network Sorcery Web Site*. http://www.networksorcery.com/enp/protocol/vrrp.htm (Dec. 9, 2002).
(6) JJB Security Consulting and Training, LLC (Oct. 31, 2002). Bastille Linux. *Jay Beale's Unix Security Site*. http://www.bastille-linux.org/ (Dec. 9, 2002).
(7) Cisco Systems, Inc. (Dec. 7, 2002). Cisco PIX Firewall Series. *Cisco Product Catalog*. http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm (Dec. 9, 2002).
(8) Paymentech, L.P. (2000). *Paymentech Web Site*. http://www.paymentech.net/ (Dec. 9, 2002).
(9) BB4 Technologies (2002). Big Brother Features. *Big Brother Web Site*. http://bb4.com/features.html (Dec. 9, 2002).
(10) National Institute of Standards and Technology (NIST). (Jan. 2002). Risk Management Guide for Information Technology Systems. *NIST Special Publications 800 Series*. (SP 800-30). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (May 11, 2002).
(11) Rudolph, Kaie (1998). Why Security Awareness? *Native Intelligence, Inc. Web Site*. http://nativeintelligence.com/awareness/whyaware.asp (Nov. 8, 2002).
(12) Hayden, Rhys (Nov. 11, 2002). Secure ID. *Rhys Haden's Technical Resource*. http://www.rhyshaden.com/ (Nov. 29, 2002).
(13) Moore, David; Voelker, Geoffrey; and Savage, Stefan. Inferring Internet Denial-of-Service Activity. San Diego: USENIX Security Symposium, 2001.
(14) Browning, Paul (Oct. 21, 1999). Sample Security Policy for Remote Access by Staff. *University of Bristol BS7799 Pilot Project*. http://www.bris.ac.uk/ISC/bs7799/remoteaccesspol.htm (Dec. 22, 2002).
(15) Dominguez, Jorge. Corporate Lockdown Procedure. Nashua, NH., (Mar. 2000).
(16) Dominguez, Jorge. Lockdown Notification Schedule. Nashua, NH., (Mar. 2000).
(17) The Internet Society (September 2002). Armware RFC Index. *Internet Assigned Numbers Authority (IANA) Special-Use IPv4 Addresses*. http://www.armware.dk/RFC/rfc/rfc3330.html (Nov. 14, 2002).