Global Information Assurance Certification Paper

Information Security Officer Training

GISO – Basic Practical Assignment

Version 1.0

Jack Radigan

November, 2001

Assignment 1 – Describe GIAC Enterprises

This section is intended to provide a brief description of GIAC Enterprises, its information technology (IT) infrastructure, and its business operations. Understanding these elements is key to defining an appropriate security policy.

Description of GIAC Enterprises

GIAC Enterprises is a leading provider of business-to-business credit, purchasing and marketing information. Our information products help businesses to reduce credit risk, find profitable customers and efficiently manage vendors.

IT Infrastructure

The IT infrastructure of GIAC Enterprises provides flexible product delivery choices to our customers and secure access to internal systems for our distributed workforce.

There are two methods of connectivity into our environment, the Internet or dedicated line. We also provide VPN technology for branch tunneling. Product delivery is accomplished via SMTP, FTP, HTTP or custom transaction services for our high-volume customers.

The following section provides an overview of the infrastructure (diagram follows):

Connectivity
GIAC Enterprises has contracted with two Internet Service Providers to minimize the risk of an Internet connectivity outage. The configuration of dedicated lines is a customer decision.

The Cisco 3600 class router is used for the Internet and dedicated lines. The Cisco 3000 VPN router provides VPN services.

All routers are configured for high-availability and proper ingress and egress filtering to prevent spoofed IP addresses as per section G5 of the SANS Top 20 List.

Firewalls
Each firewall is a pair of Nokia IP650 class machines with CheckPoint Firewall-1 version 4.1 installed.

All firewall pairs are configured for high-availability via VRRP. Additional configuration information is provided below for each specific firewall:

Internet Firewall
The Internet firewall provides network address translation (NAT) and protects the public services screened subnet and GIAC Enterprises internal networks.

The firewall is configured to support the following services for the Internet, dedicated lines and VPN connections:

- DNS lookup requests only.
- SMTP incoming and outgoing mail traffic.
- FTP incoming and outgoing will accept active or passive mode file transfers.
- HTTP/HTTPS incoming web traffic to the WebSEAL server only. Outgoing web traffic via the web proxy server only.

The following additional services are supported for the internal networks:

- SSH for remote administration.
- FTP outgoing file transfer requests only.
- Syslog to the security subnet for central logging.
- LDAP over SSL is provided for WebSEAL to Policy Director authentication.
- HTTP/HTTPS port 8080 is provided for outgoing web traffic. Ports 9080 and 9443 are used for authenticated incoming web traffic from WebSEAL to the web farm.

Extranet Firewall
The Extranet firewall provides network address translation (NAT) and protects the extranet services subnet and GIAC Enterprises internal networks. It also provides remote access for GIAC Enterprises personnel.

The firewall is configured to support the services provided by custom built applications that are present on the extranet services subnet for customers and partners over dedicated lines or VPN connections. Traffic to and from the Internet is blocked.

The firewall will pass all traffic coming from or to the VPN router that is within the address range defined for remote access.

Internal Firewall
The Internal firewall provides protection for the corporate services subnet and all internal corporate LANs within GIAC Enterprises.

The following services are supported for the corporate services subnet:

- SMTP and IMAP are provided to support corporate e-mail use.
- LDAP for directory and address book use.
- DNS lookups only.
- NFS for UNIX file services.
- Windows services for file and AD use.
- SSH for remote administration.
- LDAP over SSL is provided for WebSEAL to Policy Director authentication.

The firewall will pass the following from the internal corporate LANs:

- Web traffic on ports 80, 443 and 8080.
- Outgoing FTP file transfer requests to the Internet.
- Any traffic to/from VPN remote access address range.

Security Firewall
The Security firewall protects the security services subnet.

It is configured to allow incoming syslog traffic to the central logging system from all production servers within GIAC Enterprises. It also allows traffic to/from all firewalls to the firewall management console.

All other traffic is restricted to IP addresses that have been permanently assigned to Security Department personnel.

Web Farm Firewall
The Web Farm firewall protects all GIAC Enterprises web servers. The following services are provided:

- HTTP/HTTPS to/from the web farm. Ports 9080 and 9443 are used for authenticated incoming web traffic from WebSEAL.
- SSH for remote administration.
- Syslog to the central logging system.
- Web publishing protocols to/from IP addresses assigned to personnel authorized to publish/update web content.
- Application-specific traffic to/from the application services subnet.

Application Firewall
The Application firewall protects the applications services subnet. The following services are provided:

- SSH for remote administration.
- Syslog to the central logging system.
- Application-specific traffic to/from the web farm.
- Application-specific traffic to/from the extranet subnet.
- Application-specific traffic to/from the database services subnet.

DB Firewall
The DB firewall protects the database services subnet. The following services are provided:

- SSH for remote administration.
- Syslog to the central logging system.
- Application-specific traffic to/from the application services subnet.
- Application-specific traffic to/from the extranet services subnet.

Public Services Network
This is a screened subnet, which is protected by the Internet firewall and provides the following services:

DNS
Primary and secondary DNS servers for the external DNS are on Compaq Deskpro EN P600 desktops running OpenBSD 2.9 and BIND 9.1. DNS is configured as per the recommendations in section U3 of the SANS Top 20 List.

SMTP Gateway
Sendmail 8.12 on a pair of Compaq Deskpro EN P600 desktops running OpenBSD 2.9 provide SMTP service. Sendmail is configured as per the recommendations in section U2 of the SANS Top 20 List.

FTP Service
FTP services are provided on a Compaq Proliant 5500 server running OpenBSD 2.9.

Web Proxy
A pair of NetworkAppliance NetCache C3100 series machines provides outbound web proxy services.

WebSEAL
WebSEAL is a hardened reverse web proxy and supplied as part of Tivoli PolicyDirector 3.8. It provides authenticated single-sign-on access to GIAC Enterprises web services and is installed on a pair of Sun T-1 machines running Solaris 8.

Extranet Services Network
This is a screened subnet, which is protected by the Extranet firewall and provides the following services:

Custom Applications
Servers located in this network provide application-level connectivity between the GIAC Enterprises application back-end and the customer. The configuration of each server is implementation dependant.

Remote Network Access
The Extranet Firewall, in combination with the VPN router, provides GIAC Enterprises employees, consultants and contractors with remote access to the internal networks via the Internet.

Production Services Network
This is a multi-tiered set of individually firewalled sub-networks that provide the following services:

Security Services
This network contains the following services:

Intrusion Detection
GIAC Enterprises has deployed Snort and ACID for network Intrusion Detection. The Snort sensor machines receive network traffic via Shomiti taps that have been located at key points throughout the GIAC Enterprises IT infrastructure.

The IDS sensors are implemented on Compaq Deskpro EN P600 desktops running OpenBSD 2.9, Snort 1.8.3.

The database engine for IDS analysis is on a Compaq Proliant 5500 server with 250GB storage and running OpenBSD 2.9, MySQL 3.23 and ACID 0.9.6b19.

Firewall Management
All firewalls are centrally managed via a Sun Ultra 5 workstation running Solaris 8 and a CheckPoint Firewall-1 4.1 management console.

Central Logging
All security logging for production Windows and UNIX hosts is centrally managed and monitored via a collection of internally developed applications.

Real-time monitoring is accomplished during log entry conversion into a common format for entry into a MySQL database which is used for daily, weekly and monthly reporting.

Log data conversion and real-time monitoring is performed on four Compaq Deskpro EN P600 desktops, two run Windows 2000 Professional and two run OpenBSD 2.9. The database in running on a Compaq Proliant 5500 server with 350GB storage running OpenBSD 2.9 and MySQL 3.23.

Application Services
All GIAC Enterprises application servers are contained within this sub-network. The server configurations are application-specific based on application and operating system requirements, real-time or batch processing and criticality to daily business operations. Based on these needs, the configurations range from high-availability, hot-spare or single-server implementations on Compaq or Sun hardware. Operating systems in use are Solaris 8 for Sun hardware, Windows 2000 Server and Advanced Server or OpenBSD 2.9.

Database Services
All GIAC Enterprises non-mainframe database servers are contained within this sub-network. The server configurations are Sun E450 servers running Solaris 8 and Oracle 9i.

Internal Services Network
This network contains the following services:

Internal DNS
The primary and secondary DNS servers for the internal DNS are on Compaq Deskpro EN P600 desktops running OpenBSD 2.9 and BIND 9.1.

Corporate E-Mail
The corporate email system consists of the Cyrus IMAP server 2.0.16 on Compaq Proliant 3000 servers running OpenBSD 2.9.

File Services
Both NFS and Windows file services for desktop users are provided by a set of Compaq Proliant 5500 servers running OpenBSD 2.9 and SAMBA 2.2.

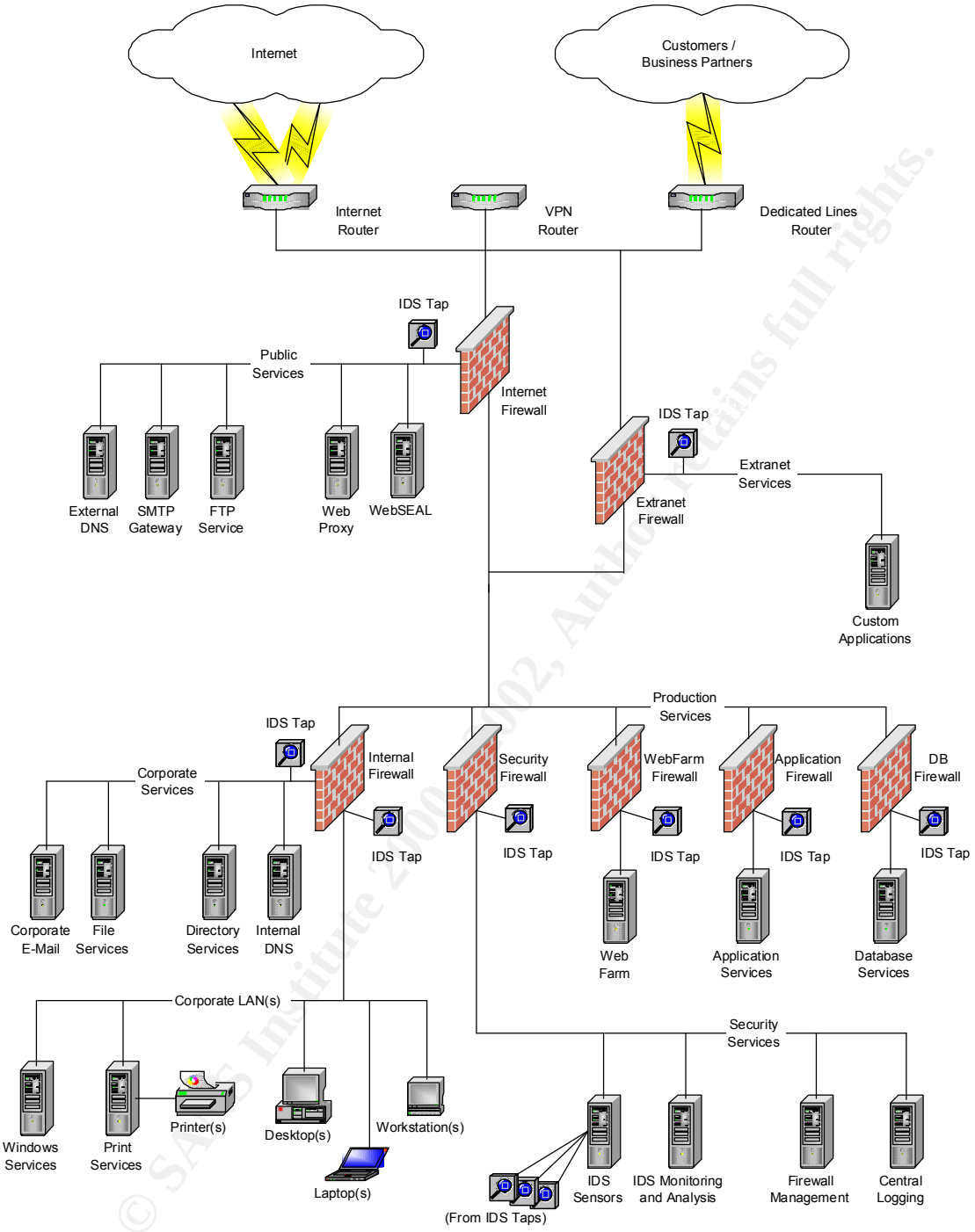
Directory Services
Microsoft Active Directory is the primary directory used by GIAC Enterprises and is implemented on a pair of Compaq ML350 servers running Windows 2000 Advanced Server.

Tivoli PolicyDirector 3.8 is used by GIAC Enterprises for single sign-on authentication to all web-based applications and services. It is implemented on a pair of Compaq ML350 servers running Windows 2000 Server.

RSA Security ACE/Server 5.0 is used for two-factor authentication with SecurID hardware tokens. It is hosted on a Sun t1 running Solaris 8.

Web Services
Web applications are hosted on either Sun Netra 20 servers running Solaris 8 with Covalent Apache 2.0 or on Compaq Proliant ML350 servers running Windows 2000 Server with IIS 5.

Corporate LANs
Each LAN is configured as per the needs of the business unit. Typical services provided are WINS for Microsoft Windows workstations and print services for both Windows and UNIX workstations.



GIAC Enterprises - IT Infrastructure

Business Operations

The following sections outline the operations and services the IT infrastructure provides in order to support the business objectives of GIAC Enterprises.

Production Operations

The following sections outline the production services and systems that are directly responsible for revenue generation:

Information Warehouse

GIAC Enterprises has built an information warehouse, which is comprised of several database systems that contains business information on over 25 million companies. The services required for maintaining these databases are:

Data Collection

GIAC Enterprises collects data from several public information services and from customers. Data is delivered on a daily, weekly or monthly basis via delivery methods that include FTP via the Internet or dedicated line and magnetic media by courier service.

Data Correction

GIAC Enterprises has developed a suite of web-based applications used by its internal and distributed workforce for the purpose of prompt data correction.

Business Analytics

GIAC Enterprises differentiates itself from its competition via a set of proprietary models it has developed. These models produce our Market Confidence Score, Creditworthiness Index and Accounts Payable Strength Ratio that our customers use to protect and enhance their business.

Business Reporting

This collection of applications generates the core business report products that GIAC Enterprises provides to its customers. A common application interface has been developed so that customers can perform ad-hoc report requests via the web, the Business Alert Service and via custom application. Each application consists of warehouse queries, information verification and report assembly modules.

Business Alert Service
This is a premium service that GIAC Enterprises provides to those customers who require immediate notification when a change occurs to one or more of their vendors or customers that could have a significant impact on their business.

Notifications are delivered via SMTP email or via custom application.

Remote Administration Tools
The following products are used for to improve the security of remote admistration production support of Windows 2000 servers:

Backlog
A free utility that converts Windows eventlog data to syslog format. This information is collected at the centralized logging system.

VNC
Virtual Network Computing is a remote administration package for Windows GUI administration. Coupled with SecureSHell, it provides a secure remote administration solution.

SSH
The SecureSHell from the OpenSSH project is used for all production UNIX and Windows servers to provide a secure remote administration solution.

Remote Network Access
GIAC Enterprises provides two levels of network access, web-only and full.

Web-only access is provided for field data workers and other users who do not need full network access to GIAC Enterprises network. It is provided via an SSL encrypted session between the remote browser and the WebSEAL proxy located on the Public Services subnet. Authentication for web-only access requires a PolicyDirector ID and a SecurID token.

All other GIAC Enterprises employees, such as remote sales, traveling employees and IT administration must use the Cisco VPN client 3.0 for full network access. The VPN session is first authenticated via SecurID token then routed through the Extranet firewall for a local LAN equivalent network session.

Assignment 2 – Define Security Policy

This section is intended to identify areas of particular risk, and define appropriate security policies and procedures to mitigate those risks.

Areas of Risk

Area 1 – Establish a Secure and Reliable Network Perimeter

A reliable and secure network perimeter is important to GIAC Enterprises, which is a network-centric company. A reliable network perimeter is required so that we can communicate with our customers, partners and employees. The perimeter must also be secure to maintain our reputation as a leading and trusted provider of business information.

If either of these qualities is compromised the overall short-term risk is the potential impact to our monthly SLAs with our customers and business partners. The overall long-term risk is to our reputation. In order to minimize these risks, the following threats must be considered and their individual risk mitigated as per the recommendations for each threat listed.

The primary threat to network reliability is the existence of a single point of failure. While it is impractical, if not impossible, to eliminate all single points of failure there are two that should be addressed.

In a network-centric environment the need for continuous Internet connectivity demands that the company not rely on a single Internet Service Provider. To reduce this risk GIAC Enterprises must maintain active connections with two ISPs at all times. Further, the two ISPs must not share the same backbone provider.

Similarly, **a**ll key network components and mission critical public services must be securely configured and implement high-availability or redundancy to reduce the risk of complete or partial outage.

Area 2 – System Component Security

Many vendors of network and general computing components supply their products in a default configuration that leans towards usability and minimizing installation support calls.

The primary threat is one of complexity by having more features than needed for the component to perform its function. Complexity and the presence of unneeded functionality can lead to sub-optimal configurations from both a security and from a reliability perspective.

The risk to GIAC Enterprises is compounded due to the number of different vendor products in use within the IT infrastructure. The consequences to the company can range from theft of service, failure to meet monthly SLAs, loss of customers, associated revenue, and lasting damage to our corporate reputation.

It is recommended that a program of system component security be implemented. The program should focus on standardized configurations that eliminate non-essential services and features not needed for the role that a given component provides.

Area 3 – Vulnerability Management

Associated with system component security is vulnerability management. Although a system may be quite secure the day it is placed into production, it will become less secure over time if appropriate remediation is not performed as new vulnerabilities are discovered.

The consequences to GIAC Enterprises may range from theft of service, failure to meet monthly SLAs, loss of customers, and associated revenue to long-term damage to our corporate reputation.

It is recommended that a vulnerability management program be established. The program would cover the effective communication of new vulnerabilities, tracking of remediation efforts and auditing to ensure known vulnerabilities do not exist within the IT infrastructure.

Area 4 – Laptop Security

GIAC Enterprises has a large distributed workforce that has been issued corporate laptops to conduct business and remotely connect to the corporate network. While laptops provide the company with tremendous leverage from a productivity standpoint, when improperly managed, they present several threats to the company.

A stolen laptop presents a tangible loss of property to the company. However, this loss may include more just then the capital costs of the unit and licensed software, it may also include valuable corporate information that was present on the system disk. Another threat to consider is to network and system security of GIAC Enterprises if the laptop can be used to gain unauthorized access into the internal network.

It is recommended that appropriate policies and user awareness training regarding the safeguarding of laptops to each associate who has been issued a corporate laptop be established.

Area 5 – Analytic Model Security

The proprietary models used by Business Analytics are strategic assets that differentiate GIAC Enterprises from their competition and are a major source of revenue to the company.

The threat of disclosure to a competitor could have an adverse impact on the company. However, that risk is considered to be a short-term consequence. A more dramatic scenario is one where the model has been altered to produce incorrect information. The consequences of this are certain and lasting damage to our corporate reputation.

As such, their protection is of paramount importance to the company. It is recommended that security policies operational procedures and audit controls be established to ensure their protection.

Security Policy

Policy 1 – Unified System Component Security Policy

Purpose

The purpose of this policy is to establish the minimum acceptable requirements for the secure configuration and proper operation of all system components within the GIAC Enterprises IT infrastructure. Adherence to this policy will minimize the risk of unauthorized access to, and disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of all information processed or stored by the system component.

Background

This policy replaces all previous versions of the following documents:

- Desktop Security Policy
- Server Configuration Guidelines
- UNIX server standards
- Firewall policy
- Web and email proxy policy
- Router configuration document

These documents contain a mix of conflicting security policy, configuration standard and guidelines, which were highlighted during a recent IT audit. As a result, IT senior management has requested the Information Security Department to review, codify and standardize these documents into one unified system security policy that will be used by all IT departments as the basis for developing standards and operating procedures documents.

Scope

The term *system component* applies to all computer, data communications and network devices that are in use within the GIAC Enterprises IT infrastructure.

Policy Statement

To ensure confidentiality, integrity and availability, all system components within the GIAC Enterprises IT infrastructure must provide appropriate administrative and technical controls in accordance with the services provided by the system component. System components are further classified and restricted as follows:

Computing Devices
All computing devices, such as servers or desktops, are restricted to data processing roles only. At no time is a computing device permitted to act in the capacity of a network layer device such as a router or switch.

The only exception to this policy would be computing devices that are deployed explicitly in the role of a network component, such as firewalls or VPN gateways.

Network Devices
All network devices, such as routers, switches, firewalls, and VPN gateways must be configured to allow only authorized network traffic through the device.

Network devices deployed on perimeter networks, such as Internet border routers, must also provide egress filtering.

In order to assist in incident forensics, all network devices must log all packets that have been dropped as per network access controls.

At no time may a network device act in the capacity of a computing device.

Responsibility

The following categories of responsibilities define the general responsibilities with respect to information security for all system components within the GIAC Enterprises IT infrastructure:

Owner Responsibilities
Information owners are the department managers, senior management or their delegates within GIAC Enterprises who are accountable for the secure operation of a given service or product offering. Each production service or product is required to have an assigned owner. The owner is responsible for designating the relevant level of sensitivity for the information processed by all associated system components that comprise the service or product and for establishing the necessary security measures to ensure the availability and integrity of the service or product. Owners also define which users will be granted access, as well as approve requests for the various ways in which the information will be utilized.

Custodian Responsibilities
One or more custodians will be in physical or logical possession of a service or product, it's associated information, and/or the system components that compromise the service or product. Custodians are responsible for safeguarding the information associated with the service or product. This responsibility includes, but is not limited to, implementing access control systems to prevent inappropriate disclosure of information, making back-ups to protect critical information from loss, and to implement, operate and maintain the security measures defined by the information owner.

Actions

In general, all system components within the GIAC Enterprises IT infrastructure must be constructed in accordance with the *principle of minimalism*. This principle refers to the removal or disabling of functionality that is not required by the system component in normal operation.

The following additional actions are also required:

1. Production Documentation
All system components within the GIAC Enterprises IT infrastructure must have accurate documentation that enables persons unacquainted with the system component to operate it. The documentation must also express the requirements set forth in this policy by providing the following minimum information:

Configuration Standard
The configuration standard document must accurately detail how a system component is constructed to ensure that the component performs all required services in a reliable and consistent manner and can be successfully rebuilt in the event of a catastrophic system failure.

Operational Procedures
The operational procedures document contains all procedures required for keeping a system component in reliable working order. Typical procedures will include, but are not limited to, user and administrative access control, information access control, data back up and recovery, troubleshooting, and general administrative maintenance.

2. Software and Firmware Maintenance
All system components within the GIAC Enterprises IT infrastructure that employ software and/or firmware to operate must, at time of production deployment, have the most recently released stable version installed. Further, during its operational lifetime, all software and/or firmware must be updated in a timely manner to ensure that risk to known vulnerabilities is minimized.

3. Non-Primary Device Boot
To ensure operational integrity, no system component may allow unprotected boot operations to occur from devices other than the primary device that was configured during production installation. This includes devices such as network interfaces, CD-ROMs, and floppy drives, etc. Booting a system component from one of these devices requires password protection.

4. Administrative Access
In order to provide an audit trail, all administrative access, local or remote, must be performed via an individually assigned an authorized user account. At no time may a generic account be used to perform administrative tasks or functions.

If the system component does not provide user differentiation as in the case of administrative access to networked devices (routers, switches, etc.) or BIOS firmware, then unique passwords must be employed for each device to limit wide-scale security compromises from occurring.

5. Anonymous or Guest Access
Every attempt must be made to limit the use of anonymous or guest access. When unavoidable, the access should be configured read-only, again, if at all possible. If administrative privileges must be associated with an anonymous account then the system component will require additional logging and intrusion detection controls which trigger alarm events when the account is used outside of established usage guidelines for the system component.

6. Unattended Time-Out
To ensure integrity, all system components must have an idle timer associated with all logged-in activities. A period of up to 10 minutes may elapse before the system component either logs the user out or activates a password-protected screen saver. When possible, this event must create a log event as well.

7. Remote Administration
All system components within the GIAC Enterprises IT infrastructure that provide remote interactive system access must do so using methods that enable and restrict all access via an authenticated and encrypted channel end-to-end. Further, the method used must provide for automatic logout or lockup of the interactive session in case the network connection is interrupted.

8. Anti-Virus Management
To ensure operational reliability, all system components within the GIAC Enterprises IT infrastructure running any release of Microsoft Windows operating system must also run GIAC Enterprises authorized anti-virus software. The A/V software must be current at production deployment and must be updated when required in a timely manner. The A/V software must be configured to begin execution at system boot time and always screen data during operation. All pattern or signature files must also be updated in a timely manner.

9. Security Logging
As required for audit or forensic investigation, all system components within the GIAC Enterprises IT infrastructure must, at a minimum, log all successful logins as well as all failed login attempts. Additional logging related to file and/or directory modification may be required as per the information owner. All security logs must be maintained in a secure manner for a minimum of 6 months. Access to logs must be protected at all times while stored on the system component. Logs must be rotated off the system component periodically and stored in a manner that provides sufficient access and modification control.

10. Synchronized Time Service
To ensure accurate time stamping of log events all system components within the GIAC Enterprises IT infrastructure must have their clock periodically synchronized with an accurate and approved time source.

11. Monitoring
All system components within the GIAC Enterprises IT infrastructure must have appropriate monitoring active in order to ensure availability of the component. Typical monitoring includes access control, network health, hardware health, and application availability. Critical systems should have configured triggers to generate real-time alarms for significant events so that the component receives immediate attention. When possible, alarms must be staged to notify for progressively worsening conditions up to complete system failure.

All monitoring must be directly relevant to the reliable operation of the system component. At no time may this include monitoring of the activities or content of an individual user who is currently accessing or has previously accessed the component without first obtaining prior written consent from both GIAC Enterprises Legal and Human Resources departments.

12. Data Storage
To minimize the risk of lost data all system components within the GIAC Enterprises IT infrastructure must employ advanced disk storage technology where available.

13. Data Backups
To minimize the risk of service outages due to system failure or data corruption all system components within the GIAC Enterprises IT infrastructure must be periodically backed up to secondary media. The information owner must develop and document a backup policy for the system component that defines, at a minimum, backup periodicity. The information owner must also define destruction and retention controls if warranted.

Policy 2 – Laptop Security Policy

Purpose

The purpose for this policy is to detail the minimum standards of protection and responsibility required by GIAC Enterprises to ensure that any risks with using laptop computers in a mobile environment is minimized.

Background

The development of laptop computers has proven to be a substantial improvement to the productivity of GIAC Enterprises associates. However, they also prevent a risk to the company if they are not handled in a responsible and secure manner.

The threat of theft imposes several risks to the company, the least of which being the loss of capital investment required to replace the stolen unit. The loss of valuable corporate information contained in the laptop system disk must be considered.

However, the greatest threat to the company is to information and network security if the stolen unit can be successfully used to establish unauthorized access within GIAC Enterprises network infrastructure.

It is for these reasons that this policy has been developed and to be adhered to.

Scope

This policy applies to all GIAC Enterprises owned laptops.

Policy Statement

Before a GIAC Enterprises owned laptop is be issued it must be entered in the asset management system. The BIOS and operating system must also have additional security controls in place to minimize the risk of compromise if the machine is lost or stolen.

Personnel who have been issued a laptop are required to safeguard the machine at all times and exercise due care appropriate to the current surroundings.

For example, it is never appropriate to leave a laptop unattended while in a public environment or to place a laptop with checked luggage while traveling. However, activating a password protected screensaver while visiting a customer premises or keeping the laptop with you as carry-on luggage would be sufficient due care.

No unauthorized software may be installed on the machine nor may changes be made to the operating system or BIOS that would increase the risk of compromise.

The GIAC Enterprises help desk must be contacted immediately for any of the following conditions:

- It is suspected that the laptop has been compromised.
- The laptop has been lost or stolen.

Responsibility

The GIAC Enterprises Desktop Support team is responsible for the secure configuration of all company owned laptops to ensure that the risk of compromise to confidential information and company network resources is minimized.

GIAC Enterprises personnel who have been issued a company owned laptop are responsible for the prevention of compromise to company information and network resources by safeguarding the laptop.

The GIAC Enterprises help desk is responsible for the prompt notification of a security compromise or loss of a company owned laptop.

Action

Laptop asset control and configuration requirements are as follows:

1. Asset Control

An asset control tag must be fixed to the bottom of the unit using a permanent adhesive.

2. Asset Management

The following information is required to be entered into the asset management system:

- Laptop make, model and serial number.
- Asset control tag number.
- Size of hard disk, memory and types of removable media components
- Power-on BIOS password (user password, not administrator)

3. BIOS and Operating System Configuration

The installed operating system must be configured as follows:

- Separate BIOS administration and power-on passwords.
- BIOS must only boot from hard disk, all other boot alternatives must be disabled.
- Password-protected screen saver that activates after 15 minutes.
- Suspend operation after 30 minutes of inactivity or when the display lid is closed.
- Require a password when resuming from a suspended state.
- Issued user cannot have local administrator privileges.

Policy 3 – Business Analytics Information Protection Policy

Purpose

The purpose of this policy is to establish the requirements for safeguarding GIAC Enterprises proprietary business analytics models.

Background

The proprietary business analytics models used by GIAC Enterprises are strategic assets that differentiate the company from the competition. They are also one of the primary drivers for revenue.

Ensuring their protection is important to the company's reputation and to the short-term and long-term corporate revenue goals.

Scope

This policy covers the use and storage of "model information" which refers to all data, program code, and supporting documentation associated with the construction, modification and use of GIAC Enterprises business analytics models.

Policy Statement

All model development and maintenance must be conducted in an access-controlled room that is restricted to GIAC Enterprises employees who have agreed to and signed an Analytics Non-Disclosure Agreement. At no time, for any reason, may this room be accessed by, or model information be disclosed to, a party that does not fit these criteria.

At no time may printed or written information related to a model be left in the open within an unoccupied room outside of business hours. All printed, written and electronic copies of model information are to be kept in locked cabinets within the access-controlled room.

At no time may copies of model information leave the access-controlled room in an unencrypted or salvageable form. Model information on media and paper must be permanently destroyed except for the express purpose of off-site backup. All off-site backups are limited to electronic copies that must kept at an approved location and be in an approved encrypted format.

Any computing systems containing model information must be configured using a company-approved standard for security hardening. Access control must employ two-factor authentication at a minimum.

All file transfers of model information must be point-to-point over an encrypted channel within the internal corporate network. Remote access outside of the internal corporate network is prohibited at all times.

Responsibility

The Business Analytics Group is responsible for developing the standards and procedures that implement and ensure the requirements for the confidentiality and integrity of all model information as set forth in this policy.

GIAC Enterprises Corporate Audit Group is responsible for reporting to senior management the results of an annual review of all model information controls and practices.

Action

The handling and destruction of model information must be accomplished in a secure manner as follows:

Media Handling
Prior to removal from the access-controlled room, all media containing unencrypted model information must be destroyed using a company-approved information destruction tool.

Paper Handling
Printing must be accomplished via a directly attached printer. Writing must be performed on a single sheet of paper against a hard surface to prevent residual impression images from being created. All paper must be destroyed using a company-approved shredder.

Whiteboards
Only dry-erasable markers are permitted for use with model information. Whiteboards containing model information must be wiped clean with an approved dry-erase cleaning solution to ensure that residual images are destroyed.

Assignment 3 – Define Security Procedures

This section is intended to use existing policy to develop operational procedures that can be used to implement and enforce that policy.

Guidelines for System Security Management

These guidelines have been written to support the implementation and adherence to the following policies:

- Unified System Component Security Policy
- System Component Vulnerability Management Policy

Overview

The increasing size and complexity of GIAC Enterprises technology infrastructure coupled with the growing number of reports in the media regarding attacks on Internet-based services serves to underscore the need for a proactive approach to minimize the risks associated with our expanding presence on the web. In order to effectively address this concern, the Information Security Department has developed a set of formalized policies and procedures for improving and maintaining the security of our networked services via a formalized process. This will include the development of security and configuration baselines, and the management of security vulnerabilities for all networking and computing components within GIAC Enterprises.

Security standards will be required as a foundation for current and future security management objectives. These will be used for evaluating vulnerability notifications, known vulnerability scanning results, audit, and forensic activities.

Problem management tickets will now be used for tracking security related issues due to an existing audit requirement that highlights the lack of a formal process for this activity. Tickets will be initially assigned to an identified Security Liaison who will be accountable for ensuring that the problem is appropriately handled as outlined in this document.

Security Liaisons are those associates with management accountability for specific technology areas within GIAC Enterprises. It is assumed that these associates will also be the first-line subject experts for their areas or will have a subject expert reporting to them.

Security Administrators are those associates who are responsible for the maintenance and operation of specific technologies within GIAC Enterprises. These associates will be responsible for performing the remediation work necessary for a given audit issue, vulnerability or exposure.

Although the Security Liaison can also be the Security Administrator who performs the work required for vulnerability remediation, a Security Liaison cannot delegate accountability for remediation to a Security Administrator. That must stay with the person who also has management accountability.

The Information Security Department is responsible for running audit scripts, the collection, assignment, and tracking of vulnerability notifications, and periodic scanning, assignment, and tracking of production network components for known exposures.

Together, Security Liaisons, Security Administrators and the Information Security Department form the foundation of a distributed security function for proactive security and vulnerability management within GIAC Enterprises.

Security Standards

The guiding principle for all security standards are to ensure that GIAC Enterprises is managed in a consistent manner with minimum risk of service failure and to make the administration of our infrastructure more efficient.

To meet this goal the following guideline has been developed to assist Security Liaisons in developing and documenting security standards for all computing and network components they are responsible for in a manner that is consistent with approved security policies.

In general, relevant security policy, security configuration best practices, and all known security related issues or flaws must be addressed in the documented standard. It should also be understood that developing a security standard is not a one-time activity. Standards will need to be updated as new flaws are discovered or functionality is added to a component.

Security standards should also be considered an addendum or appendix to any existing configuration standards already in place for production equipment. The rationale for not integrating security standards directly into a configuration document serves to reduce duplication and therefore, risk of not updating relevant standards when necessary.

Configuration Research

Although there are several procedures and scripts that can be obtained for securing a system component, these often require a layered or iterative approach that is best accomplished prior to deploying new equipment into production. Using these tools on existing production components will often leave the unit in an unusable state. Depending on the component in question and its criticality, it may be more prudent to switch the existing unit with a replacement system that has been configured with security in mind.

It is recommended that Security Liaisons begin their research at the SANS (System Administration, Networking, and Security) Institute web site. They maintain a

substantial library of documents categorized by topic; each document typically provides references to additional research that will help the Security Liaison in developing a security standard that reflects current industry best practices.

The SANS library can be found at:

http://www.sans.org/infosecFAQ/index.htm

Vulnerability Research

Addressing current vulnerabilities when deploying new equipment into production should be fairly straightforward by using the latest stable releases of firmware, software and associated patches or procedures. These, of course, should be documented in the security standard so that the assigned administrator can successfully configure the component in a secure manner.

However, when trying to address vulnerabilities in existing production systems the chore is made more complex by time constraints and the desire to not introduce instability into a system that may not be in an entirely known state of configuration.

For these situations it is recommended that the Security Liaison begin their vulnerability research using the ICAT metabase that has been developed by the *National Institute of Standards and Technology* (NIST). The metabase contains, at the time this document was written, over 2,400 of the most significant and important vulnerabilities and exposures known for over 1,200 computer, network and software products. Included in each entry is a summary of the vulnerability, a severity rating and references to patches or procedures to address the vulnerability.

The metabase will simultaneously provide the Security Liaison with a focused set of significant vulnerabilities for a given system component and details of what is required to address them. It is recommended that all high severity vulnerabilities be considered without question. In addition, medium severity vulnerabilities should be incorporated for critical systems and all components located in the DMZ network.

The ICAT metabase can be found at:

http://icat.nist.gov/icat.cfm

The following NIST bulletin details ICAT usage:

http://csrc.nist.gov/publications/nistbul/07-00.pdf

Software and Firmware Research

From a security perspective, software and firmware should be current with the most recent stable release when a component is initially deployed into production.

After deployment, the work required to keep software and firmware current after deployment is often a significant activity due to the requirements of change management scheduling. For this reason, the Security Liaison has to research new releases of software and firmware to weigh the benefits of updating the component against the work it would generate.

There are four fundamental criteria to focus on when evaluating new releases or updates of software and firmware:

Functionality
Added functionality, while technically interesting, may simply not directly benefit the business objectives that the unit is intended to perform.

Reliability
Often, a claim of improved reliability may not be directly applicable to the function the component performs in production. Can this improvement be independently measured on a test unit to quantify this claim in terms of better interoperability, uninterrupted up time, faster or more efficient processing, or similar objective measures?

Integrity
Does the upgrade improve the integrity of the component? Does the update address existing problems or bugs that can potentially introduce occasional errors?

Confidentiality
If the component performs encryption to protect data, does the firmware upgrade address an existing flaw, or add new functionality that are applicable to the function the component performs in production?

Audit Controls

In order to effectively audit a system component the security standard must contain information that can be used to conclusively determine the configured state of the device. In general, the controls should reflect relevant security policy. However, some questions to consider for developing these controls are:

- What functional sub-components are present in the system component?
- Which network services and/or processing are the component configured to perform?
- Which functional sub-components are installed but disabled?
- Which versions of software and/or firmware are installed in the system component?
- Which patches have been applied to the system component?
- Which logical access controls are in place?

Vulnerabilities

Broadly defined, vulnerabilities are flaws in computer and network hardware or software that has a known exploit available to the general public. If not remediated, the presence of the vulnerability could lead to an incident that has a negative impact to the business interests of GIAC Enterprises.

Vulnerability Notifications

In order to provide prompt notification of new vulnerabilities, The Information Security Department has subscribed to several advisory services such as CERT, CIAC, SANS and the Cassandra project managed by CERIAS.

While there is no set format for the information included in a vulnerability notification they usually contain details along the following:

- Information regarding what functions within a component that the vulnerability affects.
- The risk(s) the vulnerability presents for continued use of the component.
- What actions are required to remediate the vulnerability.

Vulnerability Exposures

If a known vulnerability exists within a production system component this is regarded as a *vulnerability exposure*. In order to ensure the security of critical system components The Information Security Department will perform regular and on-going scanning of all GIAC Enterprises networks to detect the presence of any existing vulnerability exposures within production system components.

Vulnerability Assignment

When a vulnerability notification is received or a vulnerability exposure has been detected, The Information Security Department will create a problem ticket. They will also refer to their product responsibility matrix to determine which Security Liaison the problem ticket will be assigned to. The current tool for this is an Excel spreadsheet containing over 1,200 products that are tracked by the Cassandra project.

Severity Categorization

The Information Security Department will also define a severity level for the vulnerability before assignment. Typically, notifications will have a rather straightforward description, which makes the severity level rather obvious. However, there may be situations where the determination requires a subject expert to review the vulnerability. In these cases the Information Security Department will initially assign the

vulnerability an *unknown* status for severity, which will then require the Security Liaison to review and categorize the vulnerability.

The guidelines for vulnerability severities using the 3 levels within the problem management system are detailed as follows:

Severity Level 1
This level requires immediate attention. The types of vulnerabilities that this category is reserved for are those that present an extreme risk to secure operation if remediation is not performed. Examples would be the ability to remotely execute commands or modify content via functional exploits that are publicly available on the Internet.

Severity Level 2
Vulnerabilities assigned this level typically do not directly compromise a component, as is the case with a Severity 1 problem. For example, this level might refer to attacks such as denial-of-service (DoS) that are easily activated due to the existence of functioning exploits that are publicly available on the Internet.

Severity Level 3
This level is reserved for vulnerabilities that the Information Security Department could not determine the severity level at ticket creation. The Security Liaison will need to reclassify the vulnerability upon receipt.

Vulnerability Management

Once the Security Liaison receives the vulnerability notification via the problem management system the following steps need to be performed:

1. Immediately for Severity 1 & 2 vulnerabilities, otherwise within 1 business day of receipt, determine if the ticket was correctly assigned. If not, update the ticket with the group that is responsible for the vulnerability and re-assign to that group and also notify the Information Security Department of the error so that the product responsibility matrix can be updated.
2. Immediately for Severity 1 & 2 vulnerabilities, otherwise within 2 business days of receipt, evaluate the vulnerability for applicability. For the purposes of remediation, applicability is defined to mean that the vulnerability relates to a given area of functionality that is present in the component. This also means that the vulnerability is applicable even if the functionality is not currently used and/or disabled.
3. Immediately for Severity 1 & 2 vulnerabilities, otherwise within 5 business days of receipt, develop a remediation plan to address the vulnerability. The activities associated with remediation may include pre-production testing to evaluate the impact of integrating the required changes within the production environment.

4. Immediately for Severity 1 & 2 vulnerabilities, otherwise within 10 business days of receipt, submit the remediation plan via a change management request for approval. Schedule additional activities, such as customer notification as required in order to accomplish the remediation work.
5. As soon as practical for Severity 1 & 2 vulnerabilities, otherwise within 30 business days of receipt, assign the problem ticket to an administrator for remediation of the vulnerability.
6. Update the relevant security standard once all affected system components have been remediated to reflect the configuration requirements for future system deployments of similar components.

Vulnerability Remediation

The administrator with responsibility for the remediation should review all relevant documents well in advance of actually performing the work. The administrator should evaluate the applicability of the vulnerability to make certain that possible undocumented changes to the system component have not rendered the needed changes irrelevant. The administrator should also evaluate the remediation plans developed by the Security Liaison to ensure correctness so that the risk of unanticipated problems is reduced.

Once the remediation is complete and change management impact testing has been satisfied for all applicable system components the administrator should close the problem management ticket and notify the Security Liaison.

Remediation Verification

Once the problem ticket has been closed the Information Security Department will schedule a vulnerability scan against the affected system component(s) to ensure that the vulnerability has, in fact, been remediated.

If the vulnerability is found to still exist then a post mortem must be scheduled to review the remediation plans and determine the appropriate follow-up actions to correct the situation.

References

Bernstein, Terry. Bhimani, Anish B. Schultz, Eugene. Siegel, Carol A. Internet Security For Business New York: John Wiley & Sons, Inc. 1996

Chapman, D. Brent , Zwicky, Elizabeth D. Building Internet Firewalls. Sebastopol: O'Reilly & Associates, 1995

Childers, Richard. "Laptop Computer Security" October 30, 2000
URL: http://www.sans.org/infosecFAQ/homeoffice/laptop.htm

Cresson Wood, Charles. Information Security Policies Made Easy – Version 7 Sausalito: Baseline Software, Inc. 1999

Guel, Michele D. - SANS Institute. "The SANS Security Policy Project"
URL: http://www.sans.org/newlook/resources/policies/policies.htm

National Institute of Standards and Technology. "Introduction to ICAT"
URL: http://csrc.nist.gov/publications/nistbul/07-00.pdf

King, Christopher M. Dalton, Curtis E. Osmanoglu, Ertem. Security Architecture – Design, Deployment & Operations Berkeley: Osborne/McGraw-Hill, 2001

SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated)" Version 2.501 November 15, 2001
URL: http://www.sans.org/top20.htm

Software Engineering Institute, Carnegie Mellon University. "Protect your Web server against common attacks" 2000
URL: http://www.cert.org/security-improvement/practices/p082.html

Software Engineering Institute, Carnegie Mellon University. "Securing Network Servers" 2000
URL: http://www.cert.org/security-improvement/modules/m10.html

Tudor, Jan Killmeyer. Information Security Architecture Boca Raton: CRC Press, LLC 2001

Wadlow, Thomas A. The Process of Network Security Reading: Addison Wesley Longman, Inc. 2000

Products

Andrew Systems Group, Carnegie Mellon University, Cyrus IMAP Server
URL: http://asg.web.cmu.edu/cyrus/imapd

Check Point, Firewall-1
URL: http://www.checkpoint.com/products/security/firewall-1.html

Cisco 3600 series routers
URL: http://www.cisco.com/warp/public/cc/pd/rt/3600/index.shtml

Cisco VPN 3000 series routers
URL: http://www.cisco.com/warp/public/cc/pd/hb/vp3000/

Cisco VPN Software Client Version 3.0
URL: http://www.cisco.com/warp/public/cc/pd/vpnc/vpncl/

Compaq DeskPro EN P600 Workstation
URL: http://www.compaq.com/products/quickspecs/10023_div/10023_div.HTML

Compaq Proliant 3000 Server
URL: http://www.compaq.com/products/servers/proliant3000/index-300-333.html

Compaq Proliant 5500 Server
URL: http://www.compaq.com/products/quickspecs/10279_div/10279_div.html

Compaq Proliant ML350 Server
URL: http://www.compaq.com/products/servers/proliantml350/

Covalent Apache 2.0
URL: http://apache.covalent.net/

Danyliw, Roman. Analysis Console for Intrusion Databases
URL: http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html

IBM Tivoli Software SecureWay Policy Director
URL: http://www.tivoli.com/products/index/secureway_policy_dir/

Incident Response Database Effort, CERIAS, Purdue University. "The Cassandra Tool"
URL: https://cassandra.cerias.purdue.edu/main/index.html

Internet Software Consortium. BIND 9
URL: http://www.isc.org/products/BIND/bind9.html

Intersect Alliance Backlog
URL: http://www.intersectalliance.com/projects/BackLogNT/index.html

Microsoft Internet Information Server 5.0
URL: http://www.microsoft.com/windows2000/server/evaluation/features/web.asp

Microsoft Windows 2000 Advanced Server
URL: http://www.microsoft.com/windows2000/advancedserver/

Microsoft Windows 2000 Server
URL: http://www.microsoft.com/windows2000/server/default.asp

MySQL 3.23
URL: http://www.mysql.org/downloads/mysql-3.23.html

National Institute of Standards and Technology, NIST, ICAT Metabase
URL: http://icat.nist.gov/icat.cfm

Network Appliance NetCache C3100
URL: http://www.netapp.com/products/netcache/netcache_family.html

Nokia IP650 Firewall
URL: http://www.nokia.com/securitysolutions/platforms/650.html

Oracle 9i Database
URL: http://otn.oracle.com/products/oracle9i/content.html

The OpenBSD Project, OpenBSD 2.9
URL: http://www.openbsd.org/29.html

The OpenSSH Project OpenSSH 3.0
URL: http://www.openssh.org/

RSA Security, ACE/Server 5.0
URL: http://www.rsasecurity.com/products/securid/datasheets/dsace50.html

RSA Security, SecurID
URL: http://www.rsasecurity.com/products/securid/

The SAMBA Project, SAMBA 2.2.2
URL: http://us1.samba.org/samba/whatsnew/samba-2.2.2.html

Sendmail, Inc. Sendmail 8.12
URL: http://www.sendmail.org/8.12.1.html

Shomiti Century Inline Tap
URL: http://www.finisar-systems.com/htdocssh/products/taps/index.html

Snort 1.8.3
URL: www.snort.org

Sun Microsystems Enterprise 450 Workgroup Server
URL: http://www.sun.com/servers/workgroup/450/

Sun Microsystems Netra 20 Server
URL: http://www.sun.com/products-n-solutions/hw/networking/netrat/netra20/

Sun Microsystems Netra t1 Server
URL: http://www.sun.com/netra/netrat/t1/

Sun Microsystems Solaris 8 Operating Environment
URL: http://www.sun.com/solaris/

Sun Microsystems Ultra 5 Workstation
URL: http://www.sun.com/desktop/products/ultra5

Virtual Network Computing
URL: http://www.uk.research.att.com/vnc/