GIAC ENTERPRISES – REMOTE ACCESS SECURITY POLICIES AND PROCEDURES

GIAC INFORMATION SECURITY OFFICER BASIC PRACTICAL ASSIGNMENT V1.2 (February 9, 2002)

James B. Johnson

Submitted: September 19, 2002

TABLE OF CONTENTS

DESCRIPTION

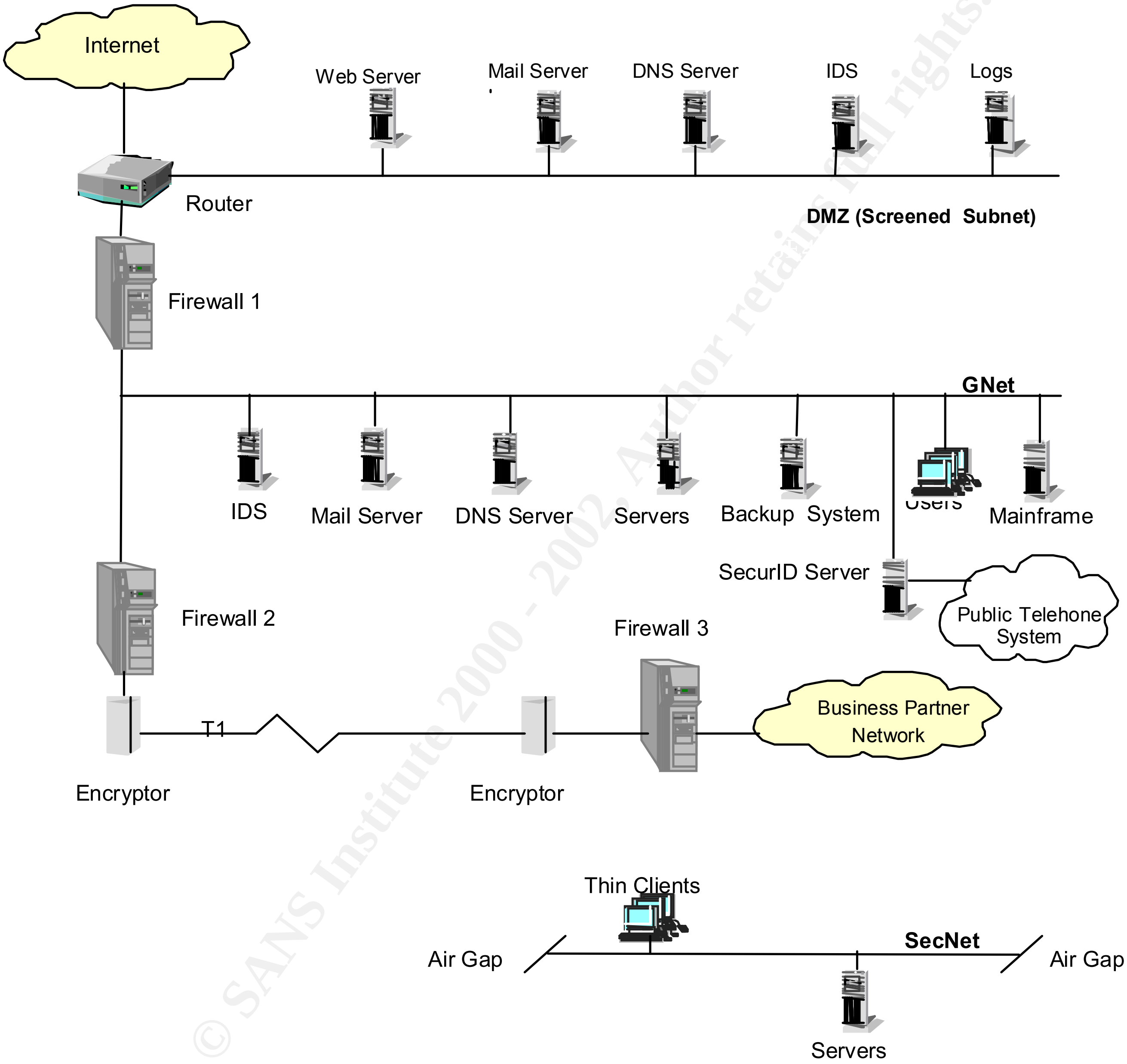
GIAC Enterprises is a corporation whose sole purpose is to manage a government-owned facility that manufactures specialty nuclear materials. These products are manufactured at one location covering 50 square miles. There is one business partner located external to the site. Due to the secrecy of the processes used to make the products, portions of the information managed are highly sensitive. (1) Being a government facility, there is also information that must be freely shared with the general public as required by the Freedom of Information Act. All employees are screened and are required to have government-issued security clearances. A full-time physical security protective force limits access to the site. GIAC Enterprises employs nearly 4,000 people. Business requirements necessitate that nearly 40 employees be on travel at any given time and that 20 of these employees have access to GIAC Enterprises Network remotely. In addition, 20 employees are telecommuters. While there is primarily one customer for GIAC Enterprises products, due to the nature of the products being handled, maintaining a very positive image of GIAC Enterprises with both the local and national community is important to the long-term viability of GIAC Enterprises.

The cyber security posture of GIAC Enterprises is in a state of transition. The old philosophy was to concentrate limited resources on having a hard external shell while leaving the network and systems inside the firewall somewhat soft and loosely managed. Based upon the increasing threats documented by the cyber security community, and evidence of increased attacks by GIAC Enterprises log indicators, GIAC Enterprises security posture is changing to defense-in-depth where:

- The firewall remains a hard shell.
- Network Intrusion Detection is being added to key locations on the network.
- Minimum security configurations are required for all systems.
- Host-based intrusion detection is required for critical systems.
- System administrators and Computer System Security Officers are receiving additional training on cyber security principles and are required to implement not only company policies and procedures but also generally accepted security practices.
- A vulnerability scanning program is being implemented even though the initial scans have been overwhelming, requiring scans to be limited to the top 20 vulnerabilities of concern.

IT INFRASTRUCTURE

A high level illustration of GIAC Enterprises Network (GNet) showing the key components of operation is shown below in Diagram 1. (2) Portions of the material presented in the diagram are from Jeff Horne's "GIAC Firewall and Perimeter Protection Curriculum SANS Network Security 2000 Practical Assignment."



GIAC Enterprises Network (GNet)
Diagram 1

Border

The border includes a router with the following configuration:

Router Cisco 7206, OpenBSD 2.8, IPfilters ver 3.4.16

The router screens traffic for the DMZ and the firewall (Firewall 1). The purpose of this router is to direct limited traffic to the DMZ and to screen traffic before reaching Firewall 1 reducing firewall traffic and logging. Though this system is being referenced as a router, it does perform some basic firewall functions. The router is kept up to date with the latest patches from Cisco. Configuration information to help prevent being utilized as a participant in a Denial of Service (DOS) attack was used from (3) www.sans.org/ddos_roadmap.htm. Blocked incoming traffic includes protocols not used such as Netbios, private IP address space, source addresses of internal systems, and ICMP. Blocking this traffic prior to the firewall filters a large sum of unwanted traffic, allowing the firewall administrator to focus attention on the remaining traffic. Outgoing traffic is screened, and inappropriate traffic such as outgoing IP packets with internal addresses as the destination and source address not within internal address space is blocked.

DMZ

(4) Major components of the DMZ, as partially extracted from Mason Richardson's "GCFW Practical Assignment," include:

Firewall 1	Sun Ultra 60, dual 450 mghz CPUs, Solaris 2.7, Symantec (formerly Raptor) version 6.5
Web Server	Sun Ultra 10, Solaris 2.7, Apache http server version 1.3
Mail Server	Intel Pentium 3 800 mghz OpenBSD, Sendmail version 8.11.3
DNS Server	Intel Pentium 3 800 mghz OpenBSD, BIND Version 8.2.3
IDS	Gateway Pentium 4 966 mghz, Windows 2000, ISS Realsecure
Log Server	Intel Pentium 3 800 mghz., OpenBSD

(5) Due to business necessity discussed later in this document, GIAC Enterprises must maintain systems in the DMZ that are more susceptible to hacker attacks than systems on the corporate intranet named GNet. To help mitigate this risk, GIAC maintains a strict configuration policy for systems located on the DMZ. All systems require a security plan approved by the site Computer Security Manager prior to DMZ connection.

- Only single-purpose servers are allowed.
- Operating systems must be robustly maintained including a minimum weekly update for both operating systems and application security patches.
- Alerts by CERT, VAVCIRT, or IAVA must be addressed by close-of-business on the day received.

- Compilers are not permitted on any systems installed on the DMZ.
- File integrity tools are required for all critical files including the operating system.
- Any code or scripts not needed must be removed including sample code and scripts.
- User accounts are maintained to a minimum and passwords for DMZ systems must never match passwords used on GNet.
- Dynamic routing is disabled.
- Host intrusion detection services logging to the external log server is required.

The firewall in the DMZ that protects GNet is a proxy firewall. GIAC selected a proxy firewall because the industry considers them to provide greater protection because the proxy firewall conducts both packet inspection and stateful inspection. The speed needed for GIAC was achieved with the hardware utilized. The firewall is configured using the principle of least privilege and is monitored 24 x 7 using alarms that trigger the site paging system. The firewall also performs NAT services for outward-bound Internet traffic to isolate internal system IP addresses from the external.

A log server is used to record activity logged by both the network intrusion detection system (IDS) and the host IDSs. A separate log server is maintained to help isolate the logs from the systems potentially being compromised. This helps prevent hackers from covering their tracks and going undetected. The IDS analysis station maintains a robust configuration being stripped, patched, and wrapped. Snort, which is available at www.snort.org, is currently being used, and SHADOW, which is available at www.nswc.navy.mil/ISSEC/CID/, is being evaluated as an additional analysis tool.

Intranet (GNet)

GIAC Enterprises Intranet (GNet) is a network that connects the majority of desktop systems and the resources that they access. This is an Ethernet network running TCP/IP with an FDDI backbone. Both DHCP and fixed IP are utilized to assigned IP addresses. A large variety of servers are attached to the network including UNIX, NT, and Win2000. Desktops used included Win95/98, WinNT, Win2000, and Macintosh.

All key systems, servers, and backups are centrally housed in a central computer facility designed with full uninterruptible power supplies (UPS), climate control, and physical security. Full backups of workgroup servers, email servers, etc., are conducted weekly (based upon the importance of the information) with incremental backups conducted daily. A contract is in place for off-site processing of the most critical applications in case of operational interruption, and live testing of business continuity and disaster recovery plans is conducted at least annually.

Though requirements for maintaining hardened systems are not as strictly enforced as for the DMZ, emphasis is still placed on maintaining minimum system security configurations, and updates are required for both operating system and application security patches monthly or as directed by Computer Security. One area of configuration that requires more frequent updates is malware protection. GIAC had a series of malware attacks including Nimba and Melissa that required significant resources to contain and eradicate. GIAC updated its policy and funded Norton AntiVirus software for all desktops and servers one year ago, and since that time no major outbreak has occurred. Most infections were caused by incoming email; now the email servers catch and eradicate the malware before it becomes a concern. Intrusion detection (ID) is employed like the DMZ. The IDS program is relatively young, and multiple network IDS sensors are being strategically placed to log the most sensitive areas of the network.

Dial-in access is allowed to GNet but only through one modem bank specifically designated for such use. Two-factor authentication is required with one being a SecurID card and the other a password in compliance with a robust company password policy. Connection to GNet is allowed only with a GIAC-issued computer, and GAIC-issued computers are allowed only to connect to GNet. All modem connections are strictly controlled and require specific approval by the Computer System Manager prior to use. War dialing is utilized frequently to detect possible modems connected to the network. Modems are considered a vulnerability area for GNet, and a new product that controls connections at the telephone switch called TeleWall is being pursued. The GNet trust model is that internal machines may not trust external machines including those in the DMZ.

SecNet

SecNet is a small thin client network of 20 clients and 2 servers. This network processes highly sensitive information regarding the techniques and compositions used to manufacture nuclear materials. This network is physically secured and separated from all other networks using hardened conduit for network wiring and vault-type rooms for system locations. Layers of increasingly intense physical security ensure that only authorized personnel have access to these systems. This includes armed guards and electronic systems that require three forms of authentication; what you have, what you know, and what you are before access is granted.

Information exchange between GNet and SecNet is highly controlled. There is no network connection between GNet and SecNet. All ports not approved for use in the security plan are physically blocked on the SecNet computer systems either being blocked permanently or by key controlled locks. A key control system ensures that two individuals are required to unlock ports when necessary to copy information. Files to be transferred to GNet are required to be reviewed by Computer Security using a company proprietary application that ensures that only the information intended was copied, that no information is contained in the file slack space, and that hidden information isn't embedded. Once the files clear Computer Security, the information is then reviewed and approved by a Classification Officer before it is approved to be copied onto GNet. Due to the complications and associated overhead costs, information is very rarely transferred between SecNet and GNet. The process for transferring information between GNet and SecNet is less stringent in that the Computer Security and Classification Officer review isn't required because information on GNet is much less sensitive that for SecNet and is approved for us on SecNet if needed.

BUSINESS OPERATIONS

GIAC Enterprises' network structure can be viewed as having three layers based upon the sensitivity level of the information being processed and the protection required for that information. These layers in increasing security requirements are: DMZ, GNet, and SecNet.

DMZ: The demilitarized zone (DMZ) hosts the systems used to interface with the general public including vendors and regulators. While the DMZ is protected from some of the risks from the Internet through the WWW router, minimum protection is provided. This area of the network is used to maintain public relations, allow vendor access to requisition proposals, and provide environmental data required for the regulators while limiting the exposure to GNet. Public and vendor access is limited to the DMZ and more specifically to the Web Server using http on Port 80. Open access is granted to allow the public to obtained generic public relations information about GIAC Enterprises. Authorized areas for vendors are password protected and this allows only authorized vendors to review requests for proposals and to submit bid proposals. While access is password protected, loss would have little impact to GIAC Enterprises continuity of operations. The information placed on DMZ systems is limited to information not considered sensitive to the company.

GNet: GIAC Enterprises Intranet (GNet) is a network that connects the majority of desktop systems and the resources that they access. This network is approved for Sensitive Unclassified Information (SUI). The majority of the 4,000 GIAC Enterprises employees use this network to conduct unclassified business operations that support the core business of manufacturing nuclear materials. Non-sensitive business operations include highly intensive maintenance programs for nuclear facilities, tracking and reporting of environmental monitoring to the Environmental Protection Agency, conducting Safety Analysis of all nuclear facilities and processes, and the normal overhead associated with any nuclear facility. Services and applications included on this network include:

Service	Application	Use
Browser	Netscape and Internet Explorer	Internal intranet and Internet searches
Office Automation	Notes	Email, calendar, routing
Desktop Automation	WinInstall	Centralizes desktop software automation
Database	Oracle	Database for applications like Payroll and PassPort
Maintenance	PassPort	Tracking and scheduling
Payroll	PeopleSoft	Track labor and produce weekly and monthly payroll
Environmental	EnvTrack (Self-developed proprietary system)	Accumulate analyze, and report environmental data

Employees are not allowed to use company resources for personal business.

GIAC Enterprises receives specific orders from one customer, the United States Government. These orders are received in paper form and are not tracked on GNet because the orders are Classified.

Access to GNet for a remote employee is supplied via a SecurID server. By using Terminal Server once logged on through SecurID, employees have access to all their accounts as if they are sitting at their workstation on-site except for files residing on their hard drive. This dial-in method is the only externally initiated connection to GNet. By policy, systems are not allowed to have another modem connection while having connection to GNet. No connections are allowed remotely from the Internet.

There is a link to GNet with an external business partner. Since sensitive information is shared, FIPS 140-1 approved Triple-DES, Cisco 3000 series Virtual Private Network (VPN) concentrators are used to provide protection of the information from sniffing and man-in-the-middle attacks. A firewall is required on the GNet side to fully protect GNet because the business partner isn't fully trusted. Services across the VPN are limited to SMTP and HTTP.

SecNet: SecNet is a small thin client network used to process very sensitive (Classified) information required in producing the specialty nuclear materials. This system is used to record orders received in either paper or removable media form from the customer and also to track orders to completion. This network is behind very tight physical security, and the two-person rule is required for access as previously discussed in the infrastructure section. This system contains GIAC's core technology and is considered the company's "Crown Jewel" because information about the processes and techniques used is highly sought after by foreign governments and terrorist organizations. Exactly what kind of information is contained and exactly how it can be used is highly secret and therefore will not be discussed in an open document.

CRITICAL RISK AREAS

GIAC Enterprises Cyber Security Department conducted a risk assessment using the method presented in the National Institute of Standards and Technology (NIST) Special Publication 800-30, Risk Management Guide for Information Technology Systems. (6) The NIST guide can be found on the NIST publication webpage at: http://csrc.nist.gov/publications/nistpubs/. Numerous threats, vulnerabilities, and associated risks were identified. After careful analysis and recommendation by the Computer Security Manager, GIAC Enterprises senior management agreed that the top three areas of concern are:

1. SecNet Compromise Outsider or Insider
2. GNet Compromise From Remote Access
3. Loss of GNet Due to Natural Disaster or Physical Terrorist Attack

These areas of concerns along with potential for damage, consequences if vulnerability exploited, risk mitigation, and acceptance of residual risk are detailed below.

SECNET COMPROMISE – OUTSIDER OR INSIDER

Overview of Threat

SecNet contains GIAC's core technology that is considered the company's "Crown Jewel." Confidentiality loss is of great concern because the technology needed to make the nuclear weapons components would be compromised. The threat-source is both foreign governments and terrorist organizations.

Before implementing countermeasures to mitigate the risk, the risk was analyzed using the NIST Risk Management Guide. The likelihood of occurrence was determined to be high because the threat-source is very well trained, highly motivated, and well financed. The impact of compromising the confidentiality of the information is considered high because it results in the compromise of National Security and ultimately may result in death to United States citizens. The resulting Risk Level is high by definition because both the Threat Likelihood and Impact are high.

Relevance to GIAC Enterprises

GIAC Enterprises' SecNet stores highly sensitive information regarding the techniques and compositions used to manufacture nuclear materials. The United States Government has entrusted this Secret information to GIAC. Compromise of this information by GIAC could result in both criminal and civil liability for the company and its employees and termination of the contract by the United States Government. Since GIAC only operates this one facility, the company would cease to exist with termination of the contract.

Consequences if Vulnerability Exploited

These secrets on SecNet are highly sought after by foreign entities and terrorists because the information could be used by foreign entities to become nuclear powers, and terrorists could use the information to develop nuclear weapons including weapons that, if used, would dwarf the events the United States experienced September 11, 2001.

Risk Mitigation

The risk must be mitigated by implementing countermeasures to reduce the likelihood that the threat will exercise the vulnerabilities to reach the target SecNet. Neither the threat nor the impact can be managed by GIAC so GIAC will focus control on the vulnerabilities to SecNet. The following countermeasures have been established to reduce the risk:

- Protecting the systems and network with multiple levels of physical security
- No external network connections (air gap)
- Strong personnel security program
- Two person rule for all media processing
- Strong password policy
- Maintaining rigorous certification and auditing program

The focus of the controls is to protect the confidentiality of the information from both the internal and external threat. GIAC considers that the implementation of the countermeasures above reduce the Threat Likelihood to low, resulting in a Risk Level of low.

Acceptance of Residual Risk

While the controls in place do not completely ensure 100 percent mitigation of risk to the confidentiality of the information, senior management is willing to accept the very small level of residual risk associated with these systems.

GNET COMPROMISE FROM REMOTE ACCESS

Overview of Threat

GIAC management is concerned about the compromise of GNet availability, confidentiality, and integrity from remote access. The threat-source is not only foreign governments and terrorist organizations; it also includes anti-nuclear activists.

Before implementing countermeasures to mitigate the risk, the risk was analyzed using the NIST Risk Management Guide. The likelihood of occurrence was determined to be high because the threat-source is very well trained, highly motivated, and well financed. The impact of compromising the availability, confidentiality, and integrity of information on GNet is considered high because it could result in impeding the organization's mission, reputation, and interests. Of greatest impact would be the compromise of the Safety Analysis system because information from that system is used in protecting the safety and health of workers and the public. The resulting Risk Level is high by definition because both the Threat Likelihood and Impact are high.

Relevance to GIAC Enterprises

GIAC relies on the availability, confidentiality, and integrity of GNET to conduct its business within the company. In the extreme case when safety related information was altered or not available and deaths to the workers or the public occurred, GAIC would be subject to both civil and criminal penalties and possible termination of the contract by the United States Government. Also of importance is the sensitive unclassified information that is processed on GNet. If the confidentiality of this information is compromised, the company is subject to both reduced award fee from the government and significant embarrassment.

Consequences if Vulnerability Exploited

The greatest consequence is if safety related information is not available or is altered so that the nuclear facilities operated are put into an unsafe state and cause a nuclear release. While it would take multiple failures within the operating facilities for this to occur, incorrect or missing data from GNet could contribute to such a scenario. This could result in death to both workers and the general public and ultimately to the demise of GIAC.

Risk Mitigation

The risk must be mitigated by implementing countermeasures to reduce the likelihood that the threat will exercise the vulnerabilities to reach the target GNet. The threat cannot be managed by GIAC so countermeasures will focus on eliminating or reducing the vulnerabilities. Risk can also be mitigated by reducing the amount of sensitive information on GNet, but, management has requested that the risk be reduced to acceptable levels while leaving all current information on GNet.

The following countermeasures have been established to reduce the risk:

- Robust Internet firewall and firewall policy
- Business partner firewall
- Network and host intrusion detection
- No external access to GNet from the Internet

- Access to GNet externally only through modem bank with SecurID
- Minimum system security configurations
- Security protection plans
- Certification of all systems
- Strong password policy
- Vulnerability scanning
- Routine and random auditing
- User code of conduct
- User awareness and computer security officer training
- Strict modem control along with war dialing to detect rogue modems.

The focus of the controls is to protect the availability, confidentiality, and integrity of GNet from external sources. GIAC considers that the implementation of the countermeasures above reduces the Threat Likelihood to medium resulting in a Risk Level of medium.

Acceptance of Residual Risk

While senior management has accepted the residual medium risk in the current configuration, they have concern over the vulnerability of rogue modems that drive the risk to medium. In accepting the current risk, senior management tasked the Computer Security Manager and the Information Technology Manager to reduce the risk to low within 90 days by implementing a telephone system firewall. While installing a telephone firewall will not completely ensure 100 percent mitigation of risk, senior management is willing to accept the remaining residual risks with the understanding that they will be updated annually on the risk profile or when any condition(s) change that increase risk.

LOSS OF GNET DUE TO NATURAL DISASTER OR PHYSICAL TERRORIST ATTACK

Overview of Threat

The availability of GNet is threatened by both natural disasters and terrorist attacks. Due to its geographical location, the information stored on GNet is susceptible to hurricanes, tornadoes, and flooding. Though more remote, the potential for earthquakes exists. An additional threat source is terrorists that may want to disrupt operations at GIAC by disabling GNet. Though thought to be a threat of little concern previously, GIAC has reclassified this as a credible threat since the centralized computing facility is near the plant border. There is one layer of physical security around the facilities that house the critical systems and major network components.

Before implementing countermeasures to mitigate the risk, the risk was analyzed using the NIST Risk Management Guide. The likelihood of occurrence was determined to be medium because the terrorist threat-source is very well trained, highly motivated, and well financed but there are some controls in place that will impede the threat. The threat of natural disaster was categorized as medium using information provided by a team of GIAC personnel with representatives from Safety, Engineering, Security, and Information Technology. The impact of both these events is considered high because it would impede the organization's responsibility of protecting the safety and health of workers and the public. The resulting Risk Level is medium by NIST definition.

Relevance to GIAC Enterprises

GIAC relies on the availability of GNet to conduct its business within the company. In the extreme case when safety related information was not available and if death or serious injury to the workers or the public occurred, GAIC would be subject to both civil and criminal penalties and possible termination of the contract by the United States Government.

Consequences if Vulnerability Exploited

The greatest consequence is if safety related information is not available or is altered so that the nuclear facilities operated are put into an unsafe state and cause a nuclear release. While it would take multiple failures within the operating facilities for this to occur, incorrect or missing data from GNet could attribute to such a scenario. This could result in death to both workers and the general public and ultimately to the demise of GIAC.

Risk Mitigation

The risk can be mitigated by reducing the vulnerability to terrorist attacks and by implementing countermeasures to reduce the impact if a disaster strikes. The following countermeasures have been established to reduce the risk:

- A business contingency plan has been established and is tested at least annually.
- A second central computing facility has been established for redundancy in an internal location several miles from the plant border. The building was engineered to withstand the strongest storm on record for the area.
- A contract is in place for off-site processing of critical applications hundreds of miles away from the site
- Full backups of workgroup servers, email servers, and critical applications are conducted weekly with incremental backups conducted daily.
- Backup tapes are stored in two separate secure locations miles apart and away from the central processing facilities
- A disaster recovery plan has been established and is tested at least annually.

The focus of the controls is to provide short-term continuity of operations during a disaster and a long-term disaster recovery strategy for returning to normal operations. GIAC considers that the implementation of the countermeasures above reduces Impact to low while the Threat Likelihood reduces to low resulting in a Risk Level of low.

Acceptance of Residual Risk

While expressing concern over the initial implementation costs and the ongoing operational cost for supporting this high rate of redundancy support, senior management was pleased with the low risk level assignment made possible by the countermeasures taken. While these measures do not ensure that a disaster won't happen, testing of both the business continuity and disaster recovery plans ensure that GIAC remains in business during a disaster.

EVALUATE AND DEVELOP SECURITY POLICY

EXISTING SECURITY POLICY

The existing access control policy below is one of the policies required to help reduce the risk of remote access compromise of GNET. Access control policy and its implementation are only a small portion of the protection measures required to reduce the risk. The policy below was used within the author's company.

Revision: 1
Revision Date: 8/1/2001

Access Control Original Signed by Site Manager

Signature: Site Manager

Identification and authentication by UserID and password are basic to access control and the protection of company intranet computing and information resources. Likewise, external dial-in access is controlled by UserID and SecurID card authentication. Company computing resources are to be used only for business related purposes and there should be no expectation of privacy. A required log-on banner at all access points is used as a notice to users.

- All individuals who require access to shared company computer systems must complete the Computer Systems Access Request (CSRF) form, or a Computer Security Manager (CSM) approved electronic equivalent, and obtain appropriate management approval.

- Access to sensitive data shall be revalidated annually by the data owner. Measures shall be in place to promptly remove access for users who change job assignments or otherwise lose "need-to-know." Failure to notify the appropriate Computer Security System Officer (CSSO) to remove a user's access may be considered a Security Incident.
- User accounts access must be re-validated annually and removed if no longer needed.
- Access to individual data items or records within an application shall be controlled at as restrictive a level as feasible – users shall be assigned the minimum level of privileges required to perform their work (least privilege principle).
- Lock-out shall occur after 3 failed login attempts where system configuration allows.
- Guest or anonymous access is not permitted on networked computers with the exception of the site's internal web, and user controlled public folders.
- Users of computers that allow others to write to shared areas shall inspect access at least annually for personal use.
- Access to the company network cannot be initiated from any public network.
- Remote access to the company intranet can be accomplished by registered users via dial-in and two-factor authentication.
- Foreign nationals shall not access company-computing resources without approval from the Computer Security Manager.
- Vulnerability scans using commercially available vulnerability tools are performed against perimeter protection whenever firewall configuration changes are made or at least quarterly.

EVALUATE SECURITY POLICY

The policy above was evaluated based upon whether the policy was clear, specific, measurable, achievable, realistic, and time-based. It was also evaluated based upon a structured format to include a purpose, scope, policy statement, responsibility, and action. The structure of the policy is very poor. The preamble to the individual policy statements includes sweeping generalizations about what is being done and does not address what the policy is nor does it provide a lead into the individual policy statements. The policy itself is too broad. Its purpose is not clear, and its scope is undefined. Responsibilities are mentioned throughout the policy; however, responsibilities are not assigned in all areas. The policy should establish who is responsible for establishing and who is responsible for approving the procedures needed to implement it. Actions are discussed for specific items, but there is no clear action identified to ensure that the policy is implemented. The item that discusses "vulnerability scans" is out of place in the access control policy statement and would be better placed in the firewall company policy. While not explicitly stated, the policy was written for a well-established computer security program and, without including a timeline, the implication is that all policies in their entirety are in effect. The policy should instead explicitly state its effective date. Distribution of this policy is not covered, and it is essential that the policy be made available to all employees.

The policy statement has some good aspects. The policy establishes the company's position on many aspects of access control while being in compliance with local, state, and federal law. The critical areas of access control such as access from any public network, remote access, and a controlled method for establishing user accounts are addressed. However, access control is such a significant aspect of policy that it should be developed into a separate policy making it easier for employees to access. The policy is forward looking and generic (not hardware- or software-specific) so that procedures can be written for company-wide implementation. The policy was current and had been approved by the site manager.

REVISE SECURITY POLICY

To preserve anonymity, the revised security policy was written specific to the fictitious company "GIAC Enterprises" as used elsewhere throughout this assignment.

Since the existing policy was too broad with an unclear scope, and its purpose not well defined, the policy needs to be revised. It needs to be split into two parts: one for remote access and one for local access. Due to its importance, this paper will focus on revising security policy for remote access to GNet. (7) A policy template from the SANS Security Policy Project, "Dial-In Access Policy" located at http://www.sans.org/newlook/resources/policies/policies.htm was used as the template for the revised policy below.

Revision: 0
Revision Date: 6/7/02
Effective: 6/21/02

REMOTE ACCESS POLICY — Original Signed by Site Manager

Signature: Site Manager

1.0 Purpose

The purpose of this policy is to protect GIAC electronic information from being compromised by remote access.

2.0 Scope

The scope of this policy is to establish dial-in access as the only permissible method to obtain remote access to the corporate network (GNet) and to describe appropriate use by authorized personnel.

3.0 Policy

Requirements

- Dial-in access is the only permissible method to obtain remote access to the corporate network (GNet).
- Dial-in access to GNet is limited to GIAC employees and third parties (customers, vendors, etc.) formally approved by department management and the GIAC Computer Security Manager (CSM).
- Dial-in access shall be strictly controlled using one-time password authentication.
- Systems used for GNet dial-in access shall be company-owned systems meeting the minimum configuration standards set by the CSM. Exceptions must be approved in writing by the CSM.
- Connection of company-owned systems to any network other than GNet is prohibited. Exceptions must be approved in writing by the CSM. Under no circumstances will simultaneous connections to both GNet and any other network be allowed.
- Accounts that remain inactive for 90 days will be deactivated.

Responsibilities

Employees with dial-in access privileges are responsible for:

- Ensuring a dial-in connection to GNet is not used by non-employees to gain access to company information system resources.
- Remaining constantly aware that dial-in connections between their location GNet are literal extensions of GNet, and that they provide a potential path to company sensitive information.
- Not attempting to connect to GNet using analog and non-GSM digital cellular phones as their signals can be readily scanned and/or hijacked by unauthorized individuals.

The Computer Security Manager (CSM) is responsible for:

- Establishing the required configurations for systems used for GNet dial-up.
- Approving the system used for one-time password authentication.
- Approving all requests for remote access.
- Routinely auditing systems used to ensure configuration compliance.
- Maintaining and updating this policy in accordance with the GIAC Policy Manual.
- Approving any and all waivers and exceptions to this procedure.
- Approving implementation procedures that implement this policy.

The Information Technology Director (ITD) is responsible for:

- Providing and maintaining the one-time password authentication system.
- Creating remote access accounts and enforcing expiration requirements.

Department Management is responsible for:

- Accessing the need for employee remote access and approving only requests that support GIAC interests.

4.0 Enforcement

Authorized personnel found to have successfully implemented the requirements of this policy during routine audits will be provided letters of commendation.

Personnel found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Revision History

6/7/02 -- The first issue of this policy originated when the Access Control policy, Revision: 1, Revision Date: 8/1/2001, was cancelled and replaced by two new policies - Remote Access and Local Access. This change was made to emphasize the need to control Remote Access.

DEVELOP SECURITY PROCEDURES

Implementation procedures are required to implement the requirements set forth by GIAC's Remote Access Policy above. For purposes of this exercise, the scenario will be that the Information Technology Manager has already installed and has operating an RSA SecurID system with a risk assessment and system protection plan approved by the Computer Security Manager. Some of the implementation procedures needed include: SecurID Account Creation, SecurID Termination, SecurID Account Request, and SecurID Audit. The implementation procedure included in this exercise will address the process required for GIAC personnel to request and receive a remote access account.

Revision: 0
Revision Date: 6/7/02
Effective: 6/21/02

SecurID ACCOUNT REQUEST Original Signed by CSM

Signature: GIAC CSM

1.0 Purpose

This procedure establishes the process for establishing remote access accounts for GIAC employees and third parties (customers, vendors, etc.) in accordance with GIAC's Remote Access Policy. This process ensures that GIAC controls the remote capability necessary to conduct business while protecting the assets on GNet by denying unauthorized access.

2.0 Scope

The procedure applies to all remote connections to GIAC's corporate network, GNet. Remote connections are only allowed through GIAC's RSA SecurID system.

3.0 Procedure

1. The line organization requesting the SecurID account completes the standard GIAC Computer Access Request Form (hard copy or electronic routing), having the end user sign acknowledging they have read and understand the Computer Security Code of Conduct and agreeing to protect GIAC assets per GIAC Remote Access Policy.
2. The requesting line organization department manager signs the Computer Access Request Form acknowledging the requestor's "Need to Know" and "Business Need" and routes the request to the Computer Security Manager (CSM) for approval.
3. The CSM reviews the request to ensure that citizenship requirements are met and that information sensitivity levels are appropriate for SecurID use.
4. The CSM routes the request to the Information Technology Computer Accounts Management (CAM) who creates the account and notifies the end user that the SecurID card is ready to be issued.
5. The end user reports to CAM in person.
6. CAM verifies that the end user listed on the Computer Access Request Form matches the personnel security badge of the employee picking up the card. If there is a discrepancy, CAM notifies management. If confirmation is positive, CAM issues the card with instructions including initial password.
7. CAM leads employee through first log-in at the CAM facility ensuring that the initial password is changed. Before leaving, the end user signs the Computer Access Request Form confirming receipt of the SecurID card and change of initial password.
8. For auditing purposes, CAM files and retains the completed documentation until the SecurID card is terminated plus 6 months.

4.0 Responsibility

CAM is responsible for reviewing SecurID Accounts annually to ensure continued need.

The CSM is responsible for auditing remote access activity to ensure that only authorized users access GNet.

5.0 References

GIAC's Remote Access Policy

REFERENCES

(1) Freedom of Information Act. URL: http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm

(2) Horne, Jeff. "GIAC Firewall and Perimeter Protection Curriculum SANS Network Security 2000 Practical Assignment." URL: http://www.giac.org/GCFW_100.php. GCFW #0089.

(3) SANS Global Incident Analysis Center. "Consensus Roadmap for Defeating Distributed Denial of Service Attacks." URL: http://www.sans.org/ddos_roadmap.htm

(4) Richardson, Mason "GCFW Practical Assignment, Version 1.5B, SANS Security 2001." URL: http://www.giac.org/GCFW_200.php. GCFW #0142.

(5) SANS Institute "Information Security Officer Training."

(6) National Institute of Standards and Technology (NIST). "Special Publication 800-30 Risk Management Guide for Information Technology Systems." URL: http://csrc.nist.gov/publications/nistpubs/

(7) SANS Security Policy Project. "Dial-In Access Policy." URL: http://www.sans.org/newlook/resources/policies/policies.htm