Global Information Assurance Certification Paper

Information Security Officer Training – GISO Basic Practical Assignment
Version 1.2

By
Vanessa A Walker

Abstract

This practical was prepared to illustrate an understanding of the course material provided for the Information Security Officer Training-GISO curriculum. This practical will identify risks and develop appropriate security policies and procedures for GIAC Enterprises. GIAC Enterprises is a fictional insurance company. I have identified three of the top security risks to GIAC Enterprises' information systems, and provided sample policies and procedures to mitigate those risks.

Table of Contents

Description of GIAC Enterprises

GIAC is a multi-line insurance company headquartered in St. Louis, MO. The company was founded in the 1930s, and has grown into the 4th largest auto, homeowner, and life insurer in the United States.

Corporate employees are located on a campus, which consists of separate buildings within a one-mile radius of each other. There are 20,000 total employees located in the corporate offices, and they provide the back office support (Claims, Underwriting, Actuary, Accounting, Legal, Investments, Information Technology, etc.) for the insurance operations. The Information Technology department at Corporate consists of 500 employees, of which 15 are dedicated to the information security function. Corporate systems support is provided and monitored 7 x 24 by the data center and help desk. There are 5,000 independent agents that make up the approximate 2,500 field offices selling personal lines insurance in every state across the U.S. The insurance industry is still very paper based, and an incorrect or incomplete application submitted by an agent can delay the issuance process greatly. GIAC has recently moved to a paperless application environment, by utilizing an electronic application, in an attempt to gain an edge over the competition.

The company maintained record profits throughout the 1990s, mainly due to the rising stock market and the insurer's investment portfolio. As the stock market has retreated and lost its momentum, the insurance industry has struggled to maintain a profitable stance and GIAC Enterprises was no exception. The severity of losses has continued to rise steeply in various parts of the country, and GIAC is looking for ways to control costs by streamlining their processes. The political environment has been very active with new state privacy legislation, and security of customer information is drawing regulatory attention. As security and privacy laws are enacted, expenses increase as GIAC complies with the laws. Expense management has become a primary focus, and the implementation of the electronic application process for the insurance product lines is helping to achieve this objective. The electronic application has become the key application on the network. It captures the customer data and transmits the required information to the back office operations to underwrite, approve or decline, rate, and issue the customer's policy. As the Enterprise Application has become critical, the availability of the network has increased in importance. The efficiency at which GIAC can process the application provides a competitive edge.

IT Infrastructure

GIAC Enterprises has standardized its software around Microsoft. For corporate employees, the internal Ethernet network for GIAC Enterprises begins at the desktop with HP workstations and IBM laptops running Windows 2000 (SP3) OS and Microsoft Office 2000 Suite. Employees log on to the internal network by using a unique user id and 8-character password. Typical servers accessed by corporate employees in their daily operations are the Microsoft Exchange Mail Servers, Application Servers (including the Enterprise Application Server), Intranet Servers, Proxy Servers, Windows

File and Print Servers, Web Mail Servers, Internet Servers, and the ADSM Network Storage Manager Backup Servers.

Norton Anti-Virus Corporate Edition is installed on all servers and workstations. Virus signatures are updated within 48 hours on the servers, and delivered or pushed to most client computers through Microsoft's SMS software. MIME Sweeper checks e-mail that is sent via the Internet. The application and database servers provide the backend infrastructure for data and core business processing. The Windows 2000 servers house applications, the IBM AIX and HP-UX servers house transactions and imaging, and the IBM Mainframe houses the auto, homeowners, and life legacy applications, production jobs, and databases. Traffic flows to the workstations from Cisco switches. Packets are routed to the switches from Cisco routers running Cisco's IOS operating system.

The internal network sits behind a Nokia IP530 firewall running Nokia IPSO software. An intrusion detection system from Internet Security Systems sits inside the firewall to monitor the activity inside the internal network. This network-based IDS will capture and analyze network packets on the internal network, and alert HP OpenView of attacks or abnormal behavior. The intent is to prevent damage by users who misuse their privileges or by users who obtain increased privileges that they are not authorized to have by increasing detection of attacks or pre-attacks.

With a documented business case and management approval, employees are provided dial up access from their laptops. Employees are allowed CD LAN dial up access (PSTN) into the corporate network via Windows Dial-Up Networking into the Windows 2000 RAS that uses LDAP queries for authentication to the network. Remote access policies are used to determine whether to accept or reject a connection attempt. Policies include rules to grant or deny access based on time of day, day of the week, group user belongs to, the machine that is attempting to connect, and the type of connection. By default, users are allowed 7 x 24 access unless special circumstances exist so rules enforcing time of day and day of the week are superficial controls. Dial-up users connect as part of the corporate network, and gain access to all network resources and services as if they were in the office. Employees are also provided access to the internet to perform necessary business activities, and a proxy server is utilized to mask the internal IP addresses. The proxy server intercepts outbound traffic, filters the traffic, and then moves it to the firewall for delivery. Data access to information on servers in the network is handled by data owners and IT security through a form approval process and is protected by unique ID and password. Employees must complete a business case form requesting access, and approval must be obtained from the manager of the business area that owns the data and the technology area. A Radius server sits on the corporate network for user id and password management services. GIAC employs role based access controls adhering to the principle of least privilege. GIAC enforces an eight-character password policy, requiring upper and lower case, alphabetic, and numeric characters. Passwords are forced to change every 30 days. HP OpenView software is utilized to monitor the logs of network activity. The application server running the OpenView software and logging the events is housed in a

secure location in the computer center at corporate. The logs are accessible for review from a console in the secured network control center.

The remote agent offices have a basic corporate configuration, since the hardware and software is a standard provided by GIAC Enterprises. Agent offices are an extension of the corporate network through a T1 leased line; the response time delay is the noticeable difference. The agent is provided an IBM laptop and staff members are equipped with HP workstations. A Windows file and print server is located in each agent's office. Typical network servers accessed by agents and their staff in their daily operations are the Microsoft Exchange Mail Servers, Application Servers (including the Enterprise Application Server), Intranet Servers, Proxy Servers, Windows File and Print servers, Web Servers, database servers, corporate mainframes, and the ADSM Network Storage Manager Backup Servers. A Cisco switch sends traffic to the Windows workstations and the file and print servers located in an agent's office. A Cisco router running Cisco's IOS operating system routes packets to the switch. The remote agent offices are connected to the GIAC network through leased T1 lines connected to a Cisco router running Cisco's IOS operating system. All agents, not staff, are provided CD LAN dial up access (PSTN) into the corporate network via Windows Dial-Up Networking into the Windows 2000 RAS that uses LDAP queries for authentication to the network. The same remote access policies used for corporate employees are used to determine whether to accept or reject a connection attempt. Dial-up agents connect as part of the network, and gain access to all network resources and services as if they were in the office.

Between the internal Nokia IP530 firewall running Nokia IPSO and the external SUN firewall running Check Point VPN-1/FireWall-1 software sits the DMZ. Just inside the external firewall sits another Internet Security Systems intrusion detection system to monitor the activities in the DMZ. It is important to monitor the activity in the public portion of the network. Connections that bypass the firewall, new threats that are not recognized yet, and viruses that sneak into the network must be detected. The IDS runs continually, is fault tolerant, resists subversion, is difficult to fool, logs events and then sends alert messages to the administrator. If abnormal behavior occurs, the administrator will be notified. The DMZ houses the IBM web servers running Windows 2000. Service providers and third party vendors who need to transmit or receive data with GIAC Enterprises enter from the internet to a Cisco router with Cisco IOS running a firewall feature set. The router will route them to the firewall. Their browser, I.E. 6, opens a 128-bit SSL connection. Business partners utilize http protocol to connect to the designated web server at GIAC, and then they are required to logon to the FTP server. Service providers transfer data, through FTP port 21, to the web server or download data from the web server through the 128-bit SSL connection. The GIAC Enterprise Application server components would set up a similar session to retrieve or deliver a file to the web server for a particular vendor.

Network Components

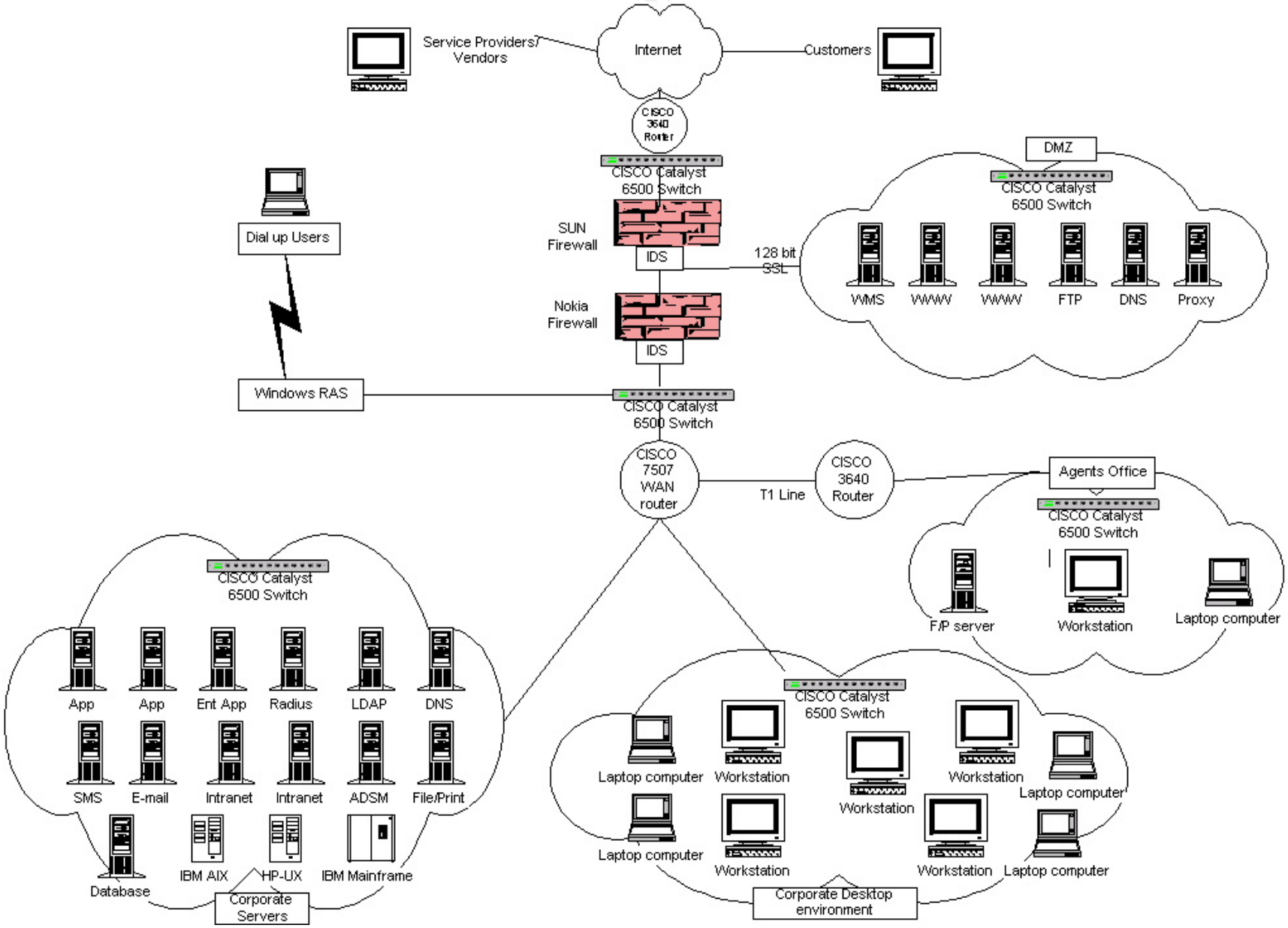
Hardware	Man.	OS Version	Product Version

7507 WAN Router	Cisco	Cisco IOSv12.2	

Network Components continued:

Hardware	Man.	OS Version	Product Version
3640 Routers	Cisco	Cisco IOSv12.1(5)T	
Catalyst 6500 Switch	Cisco		
External Firewall	Sun	Solaris8	CheckPoint VPN-1/ Firewall-1
Nokia IDS Appliance(2)	Nokia	ISS	RealSecure 6.5
Internal Firewall	Nokia	Nokia IPSO	IP530
Web Mail Server	IBM	Win 2000(SP3)	IIS 5.1
Internet Web Servers	IBM	Win 2000(SP3)	IIS 5.1
FTP Server	IBM	Win 2000(SP3)	IIS 5.1
DNS Server	IBM	Win 2000(SP3)	IIS 5.1
Proxy Server	IBM	Win 2000(SP3)	IIS 5.1
SMS Server	IBM	Win 2000(SP3)	SMS 2.0
Application Servers	IBM	Win 2000(SP3)	
Enterprise App Server	IBM	Win 2000(SP3)	
Radius Server	IBM	Win 2000(SP3)	
LDAP Server	IBM	Win 2000(SP3)	
DNS/WINS Server	IBM	Win 2000(SP3)	
Database Servers	IBM	Win 2000(SP3)	DB2, SQL
E-mail Servers	IBM	Win 2000(SP3)	Exchange Server 5.5
Intranet Servers	IBM	Win 2000(SP3)	IIS 5.1
ADSM Server	IBM	Win 2000(SP3)	ADSM 4.2
File/Print Servers	IBM	Win 2000(SP3)	

See next page for Network Diagram.



Business Operations

Agent Environment
The GIAC independent contractor captive insurance agent is the key marketing, sales, distribution, and service point for the insurance products offered by the company. Agents are the touch point to the customer, and the initiation of the customer into the company. Although GIAC Enterprises has a web site providing information on their products, customers interested in purchasing a product are referred to a local agent in their area. They cannot purchase insurance on line, and the web site is for information purposes only. The key business operation begins when the agent completes an electronic insurance application with the customer. The agent initiates the ordering of any necessary tests through the on line application, and initiates the requests for obtaining additional information from third party business partners. The electronic application contains input validation checks, and the agent must complete all required fields to move through the application to completion. This has eliminated timely delays and the need to obtain additional information from customers due to an incomplete application. Before the agent takes an application with a customer, he has previously inspected the property to be insured, and has determined the object is an insurable risk.

To obtain access to the Enterprise Application, the agent launches his Internet Explorer 6.0 web browser and provides his user id and password. On the Intranet home page the agent clicks on the Enterprise Application link. The user name and password is forwarded to the radius server using API calls, and will validate the agent for the application with their particular role, and grant them authorization to use the application. The system utilizes a three-tiered architecture. The architecture consists of the front-end Intranet server, mid-tier application server, and the back-end databases that house the critical data. The application resides on a mid-tier application server on the private portion of the corporate network. It is a proprietary application that collects information with full integration into backend legacy systems, providing a single point of integration. The application process provides a workflow approach. It prompts the agent with screens, intervenes for scheduling an exam or ordering information from a third party vendor, communicates with processes, flows from one line of business to another, and connects to the backend database. Business rules are placed on the application server and changes made to the business rules are reflected immediately. If the agent requested pictures of the property to be scanned into the network, the application server connects with the imaging server to tie the image to the application. Components of the application server build a name and address file and deposit it on the web server in the DMZ for applicants where additional data is needed from a third party vendor. The components format the file for each specific vendor based on the type of application being submitted. The file is created four times daily. Third party vendors access the web server four times daily to provide data on the applicants previously requested and to pick up the new request file. The server components also extract the information from the file retrieved from the Web server in the DMZ and obtained from the third party vendor.

The fully complete application will show up in an underwriter's work queue ready to be worked. The underwriter receives the application electronically and makes an underwriting decision. If the policyholder is approved, the application will be marked. The application utilizes rating tables to assign a premium to the policy. Once the price is obtained from the tables and determined on the system, a policy is produced and printed in the corporate office and sent by courier to the agent. The agent personally delivers and explains the policy to the customer. The premium for the policy is accepted at delivery, and the policy origination process is complete and the policy is binding. Once the electronic application is marked "approved" by the underwriter, assigned a premium, and produced for delivery, the application server component extracts the information from the completed application and the policyholder master file entry is created or updated with the policyholder information during batch. A file, containing an agent's particular book of business is updated and transmitted to the agent's local server nightly. Many agents place their book of business on their computer hard drive. This provides the agent the opportunity to access their book locally, while out of the office or in case of network problems. Changes made locally will validate and synchronize the next time the agent connects to the network. Good backup procedures need to be followed and enforced due to the amount of information stored on an agent's hard drive.

The electronic application cuts two weeks off of the processing cycle from start to finish. The electronic application is key to GIAC's streamlined business operations. The availability of the network to support this operation has become a vital component to maintain a quality customer relationship, and a competitive edge in the industry. The information captured on GIAC's customers is considered to be the crown jewels of the company. GIAC is focused on the protection of its customer records.

Agents for the company are independent contractors, and they own or lease their own office buildings as a small business owner. They are responsible for all aspects of managing their business operations. Unfortunately, physical accesses to most of their buildings involve minimal security, and GIAC Enterprises highly recommends and helps to subsidize their purchase of a security system. Past history suggests that only the agents that have had a theft occur in their office are the ones purchasing the security system. The majority do not feel the need, and do not want the extra expense. GIAC Enterprises provides the computer hardware and software for the agent's office. The equipment follows the company standard, and is preconfigured when installed in their offices. The standard configuration does not allow users to change configuration settings. Microsoft's SMS software is used to check the hardware for unauthorized software, and to provide software updates and virus signatures to the workstations in a timely fashion. The agents sign an automation agreement with GIAC, outlining their responsibility to comply with GIAC's information security policy, standards, and guidelines. The policy manual is accessible on the Intranet by all associates. The agreement also defines GIAC as the owner of the customer data and all information resources provided to the agent. Agent's offices are directly connected to the corporate internal network through T1 leased lines. The key infrastructure elements located in the agent's office were described above in the IT Infrastructure section. Agents and their

staff need access to the network to enter a new application, follow it through the processes to the point of issuance, as well as to maintain the policy on an on-going basis after issuance. Access requirements are limited to a unique user id and eight-character password. The system forces a password change every 30 days.

Corporate environment
Physical access to all corporate locations are secured with badge readers and revolving security doors. Individuals without a badge are allowed entry through one door that leads directly into corporate security. These employees or visitors are logged in and out, and provided a colored temporary badge. All individuals are required to display their badge at all times while on the property. All corporate employees have network access rights based on their role in the organization. They require network access to provide the back office support needed in underwriting, rating, issuing and maintaining an insurance policy. The connection between the agent and the corporate office is key. Critical information on a customer flows through this connection. The application server where the Enterprise Application resides assigns tasks to corporate employees based on their role in the organization and the steps in the application process. The employee expects to receive the information from the application in a timely fashion, and works hard to turn his share of the process around within specified time constraints. Employees are notified through e-mail of an entry into their work queue. Employees launch the Enterprise Application with their browser to review the policy application information and to complete their tasks. The user name and password is forwarded to the radius server using API calls, and will validate the employee for the application with their particular role, and grant them authorization to use the application. Other typical servers accessed by corporate employees in their daily operations are the Microsoft Exchange Mail Servers, Application Servers, Intranet Servers, Proxy Servers, Windows File and Print Servers, Web Mail Servers, Internet Servers, and the ADSM Network Storage Manager Backup Servers. Employees also require access to the host system where legacy applications, production jobs, and databases are stored. A few corporate employees will need access to the FTP servers located in the DMZ to monitor and support the transmission and receipt of customer information provided by third party vendors to assist in the underwriting and rating process.

Access to the internal network requires a corporate employee to log on with a user id and eight-character password. GIAC Enterprises has role based access controls and follows a "least privilege" philosophy. Employees, agents, and agents' staff are only granted rights and allowed access to the information required to perform their job functions. Timely removal/change of a transferred employee's access rights, or removal of dormant user ids has been an on-going problem for GIAC. Generally only upon a hostile termination does the user id get removed from the system and the access rights get eliminated. It is a common notion that the longer you work for GIAC, the more access rights you will accumulate. Many corporate employees require remote access to the network and all of its services and resources. With a documented business case and management approval, employees are provided dial up access from their laptops. This allows field employees to service policies while away from the office, and allows employees to telecommute. As stated previously, this is accomplished through dial up

modem connections from a laptop, and users are authenticated using their unique user id and password.

Service providers and third party vendors need to receive and transmit personal information about consumers to GIAC Enterprises. Legislation requires that GIAC protect this information, and maintain its policyholders' privacy rights. Some examples may include transmissions with the Department of Motor Vehicles, clearinghouses, credit bureaus, health care providers, and parametric services. Third party vendors access the Web Server four times daily during their batch processing. These business partners authenticate to a specific Windows 2000 FTP server in the DMZ using a 128 bit encrypted SSL session to transmit or receive information. Business partners utilize http protocol to connect to the designated web server at GIAC, and then they are required to logon to the FTP server. The access control list on the server is narrowly defined, and all default settings have been removed or locked down. The third party service provider authenticates to the server by providing a user id and password. Approved vendors are provided with a key to digitally sign all files placed on the FTP server. GIAC Enterprises purchase the keys from a certificate authority. The vendor creates a one-way hash of the message and encrypts it. To validate the integrity, the file is unlocked, decrypted, and a new one-way hash is created and compared to the one that was inside the digital signature. If the two are the same, the message has been unaltered. The Enterprise Application server components also use an encrypted SSL session and digital signature when transmitting and retrieving files, utilizing http protocol to connect to the designated web server in the DMZ. This adds security to the file while in transit and at rest. Contractually, all service providers and third party vendors are required to sign nondisclosure agreements with GIAC before any activity/discussions take place. When an agreement is reached to conduct business with the service provider or third party, a standard security clause is included in the contract language of the master agreement to protect customer data. Annual reviews of SAS-70 reports are conducted by GIAC to evaluate the security procedures followed by service providers.

Identify Risks

The three critical areas of risk to the organization have been identified. They consist of: an integrity and confidentiality loss due to theft of equipment located in an agent's office, integrity loss due to disgruntled employees or disgruntled agents' changing customer records, and an availability loss due to an attack from malicious code.

Agent's Office
GIAC Enterprises faces the risk of having the company's computer equipment stolen from an agent's office. The Human Firewall Council states on their home page at http://www.humanfirewall.com "while theft of a laptop computer that's loaded with company secrets can happen in the airport, it's just as likely to happen from your office overnight." (Human Firewall) Physical security is the foundation of any security program, and adequate controls are lacking at the agent's offices. The typical agent's office has window and door locks, exterior lighting, a computer closet, and nothing more. Agents generally provide all staff members with a key to the office. Their

employee count is minimal, and that provides flexibility in the agent's schedule. Agents do not have locking cables for their desktop hardware or laptop, but the office router and print and file server is located in a separate room with a lock.

There is a lack of understanding and awareness that the computer equipment contains the "keys to the kingdom" for the enterprise and to the agent's book of business. The company would suffer a loss for the value of the equipment stolen, but a larger cost would come from the value of the data obtained by the theft. GIAC customer records are critical to the operation of the business, and considered the crown jewels. For convenience, agents generally house their local book of business on their hard drives. Some of the information obtained from customers and collected is personal, non-public information. The sensitivity of the data the organization is trying to protect is high. The compromise of an agent's office and resulting hardware theft would be detrimental to the company and to that respective agent. "A theft of hardware causes a denial of service (you cannot use the machine if it has been stolen), a disclosure of information (the information on the system is out of your control and available to anyone who gets access to the machines), and loss of information (if the information existed only on the machine it is gone – generally forever)." (Pipkin, 2000, p. 63). Once the thief obtained the hardware from an agent's office, the information gleaned off the equipment could be used in a variety of ways. The information could be sold or given to a competitor, and the local agent and the company's business would suffer. Depending on the time it takes between when the incident occurs and when it is recognized or reported to GIAC Enterprises and accesses are removed, the workstation password could be easily cracked, dial-up networking could be started, and access to the network could be obtained. All of the company's customer information would be vulnerable, not just the agent's book of business. Customer records could be altered, copied, or stolen. For marketing purposes alone, the customer records would fetch a large price tag on the open market. If personal non-public customer information was divulged, the company could face criminal and civil penalties for not protecting the sensitive information. A lawsuit would result in legal expenses and fees for the company. Proprietary information gleaned from the equipment could cause the company to lose its competitive edge, and generate negative publicity. Customers will lose their faith in the company's ability to protect them and their information. The negative publicity and brand tarnishment that would result from a breach would have detrimental affects on the company. The reputation of the company would be in jeopardy.

Mitigation steps
There are several mitigation steps that can occur by the agent and the company.

1. The agent must begin by implementing adequate physical security controls in the office to prevent theft. The purchase and implementation of an alarm system for the office will help with deterrence and detection. The security system should be equipped to notify local law enforcement of a break in to increase the response time for notification of an incident. The posting of "secured premise" signs on windows and doors will promote basic deterrence. The agent should investigate

and implement, where appropriate, additional security options such as window bars and motion detectors.

2. Controlling the access to all critical hardware assets should be enforced. The room housing the file and print server should be inconspicuous, with a solid door that is lockable. The agent should limit and monitor access to the room, keeping a log of all technicians performing service.
3. The agent should create a checklist, used quarterly, to assess the physical characteristics of the building. The checklist should focus on the working condition of perimeter lighting, doors, windows, locks, keys, etc. Maintenance of keys to doors and windows should be scrutinized, and new locks should be purchased if a key is lost or compromised.
4. The agent needs to hold a training session for his staff to discuss physical security, its importance, and everyone's role in the office. They need to understand how physical security relates to network security and the importance of protecting information assets. A procedure should be created for opening the office each morning, inspecting the surroundings, and signaling "all clear" to employees as they arrive. The first individual to the office each day should scan the external perimeter, enter the building and scan the interior for any instances that may have occurred over night, and then place an "all clear" signal in the window for other staff members to recognize upon their arrival. If the "all clear" signal is not in view when subsequent members arrive to the office, procedures should instruct staff members to not enter the building, and to call the office for clarification. Procedures for reporting incidents should be clearly documented and communicated to staff members during the training session.
5. A record of all computer equipment should be created including the manufacturer, model and serial number. All equipment should be permanently labeled in an easily identifiable way. Equipment should also be labeled on the inside to show clear ownership. Anti-theft cabling devices should be connected to all workstations and laptops. The more difficult you make it for a thief, the less likely you are a target and the less likely they will succeed. GIAC Enterprises should provide the anti-theft cabling as a standard with the equipment provided, and instruct the office on its proper use. This will make it more difficult to remove the equipment, and will bide some time until authorities can respond to an incident.
6. Procedures should be created for when an incident occurs. Agents should create a call tree for employees, providing them with corporate areas that need to be notified, and describe what information is needed for reporting purposes. Relationships with local law enforcement agencies need to be established and discussed prior to an incident to help increase response time, and gain an understanding of the investigation process.
7. The current form of static authentication should be increased to provide additional protection against an attack. The user id provided to associates is displayed publicly, so the only protection is the hope the thief cannot obtain the password. Password cracking tools are readily available. Multi-factor authentication provides at least two ways to authenticate to the system, so a smart card and a password could be utilized. Dynamic authentication could also

be incorporated. Dynamic authentication creates a per-session authenticator, and changes with each session. (Grance, Myers, Stevens, 2002, p. 12)

8. An encryption strategy could be implemented by GIAC for data stored on a computer's hard drive. This would protect the sensitive data on the machine if the machine was obtained illegally, and would prevent customer records from being resold to competitors, copied, or altered.

Disgruntled Employee/Agent

GIAC Enterprises also faces the risk of having disgruntled employees/agents sabotage the network. In order to control expenses in the last year, GIAC Enterprises has had employee lay offs, renegotiated agent's contracts, and cut several benefit programs for employees. Morale has been decreasing among employees and agents. The company renegotiated a lower commission percentage on the agent's contract, and has halted or limited sales for certain products that were not profitable. This directly affects an agent's commission payment. This activity has prompted individuals to seek revenge by intentionally misusing the computer systems and data. A vulnerability exists throughout the network due to the lack of maintenance around security privileges once an employee transfers to a new area, or user ids become dormant. An employee can exploit this weakness and obtain access to critical data they no longer have a business need to know. Utilizing a dormant user id an employee cannot only exploit this vulnerability, but they can do it almost anonymously if they know the password or have the password reset. Leaving dormant ids active on the network can allow very sensitive data to be at risk for manipulation or disclosure. This is a big concern to GIAC for several of the same reasons mentioned regarding theft of a company computer. Insiders can also steal trade secrets and sell confidential information, which would result in a breach of confidentiality. With the current regulatory activity around privacy and security, the company can face large penalties and fees if a breach occurs of customer's sensitive information. A new law in California requires a company to notify their customers if a breach occurs from unauthorized access, and allows customers a private right of action against the company. A breach is currently defined in this law as an internal or external person with unauthorized access. This would be very detrimental to a company's brand and reputation. The company could be found to be "negligent" because of the lack luster maintenance practices, and this would ensue legal battles in the court. I feel insiders are more likely to corrupt data, and this creates data integrity issues. If the data becomes suspect, altered by an insider, business decisions made using the data are flawed. Product pricing could be calculated incorrectly, exclusions and endorsements could be added or removed, incorrect reserving could occur, and hedged investments could have the wrong maturity and amount associated with them. GIAC calculates the rates on its products based on the customer information obtained, and data altered by an insider can directly affect profitability and the competitive environment of insurance. If an agent changed the type of insurance applied for or changed the premium charged to gain a larger commission, an incorrect risk would be underwritten and a financial hardship could result. If a malicious insider added or deleted beneficiaries in a policy, a policyholder's heirs could be financially hindered. If a policy's face value was changed, the company could be liable for amounts in excess of the value of the property and the company could quickly become financially strapped if

this occurred with many policies. Insiders have the potential to be extremely lethal because they are usually very familiar with the network and know where the critical information is stored and what security precautions are in place. With the appropriate access, they can cause damage quickly, which may go undetected. The customer records of the company can become compromised, and their value to the organization will be diminished. A disgruntled employee or agent who sabotages the system could lock particular users out of the network, send embarrassing broadcast messages to users, alter accesses, defame the company's web site, reconfigure devices, and corrupt information. Depending on the insider's level of access, the damage can be very extensive. Insiders could potentially have access to hardware, software, data, storage mediums, etc., so their reach can be wide spread.

Mitigation Steps

The company has several steps that it can implement to prevent, detect, and respond to the changing of customer records by a disgruntled employee.

1. The company should do a background check on all job applicants to help assess the quality of new hires. During the orientation process, all new hires should read and be educated on the Code of Conduct form and the Enterprise Information Security Policy. These forms clearly define the ethical expectations of employees and their use of information assets at GIAC. Each employee should complete a signed acknowledgement.
2. Establishing network rights and privileges require completion of the Access Request form, business area supervisor approval, and approval from the systems technology area manager. Role based access controls enforcing the least privilege concept should be implemented and maintained in accordance with the Enterprise Security Policy. All employee network access controls need to be reviewed on a semi-annual basis, and the supervisor should revalidate business need. Business and Technology supervisors should receive and review monthly reports showing the access their employees have been granted and currently maintain.
3. Procedures must be established and followed for the update, change, and deletion of access controls. When an employee is terminated or transferred, privileges should be evaluated and halted immediately and company hardware assets retrieved. It is the responsibility of the business area supervisor to notify the technical area manager when an employee is terminated or transferred by completing the Access Removal/Change request. Dial-up access may also need to be halted.
4. Monthly reports of dormant user ids on the system should be created and sent to business area and technology managers for cleansing. Reports showing carry over dormant ids from the previous month are sent to business/technology directors for immediate resolution. An audit report finding is sent to the executive office if the same ids appear on the third monthly report.
5. Quality programming techniques incorporating field validation checks and rules can limit the range that data can be altered or manipulated. Flags can be activated for change thresholds, with notification to the systems monitor.

6. Monthly reports should be created to indicate Change/Delete records. One copy should be sent to the agent of record, and one copy should be sent to the Operations manager in corporate. Reports must be verified, signed, and returned to auditing before the next monthly reporting occurs. Computer investigation team is notified and activated if deadline passes.
7. Creation of a sound password policy and the subsequent enforcement methods are important. In accordance with the Security Policy, GIAC should enforce password changes every 30 days. The Systems area should implement a tool to force password changes across the enterprise. This will deter an employee from using someone else's password to gain access to inflict damage on customer records. Voice recognition could be implemented for password resets also.
8. GIAC Enterprises needs to establish a policy to label commonly accessed files as "read only" so they can't be altered or copied.
9. An effective firewall and intrusion detection system can help mitigate the risk of inside intruders. Procedures for patch and release management will also help in combating attacks. By using both network and host based intrusion detection devices behind a firewall, as well as an integrity checker like Tripwire, you can validate the integrity of the system and the information on the system. The firewall should log connections going outside of the company, and how much data was transferred, including e-mail. Using a security console to bring all of the information to one spot will assist in the monitoring activities, and will help spot anomalies. It is very important that devices have logging turned on, and traffic is being monitored.
10. GIAC needs to educate users to never leave their workstation unattended without invoking Ctrl+Alt+Del to lock their workstation. This will deter a disgruntled employee from using a coworker's computer to change company records. This will also assist in the tracking of malicious activity to the appropriate individual.
11. Controls and procedures should be created around removable data, and proper records handling of company information must be in place and enforced. Records management policies must be followed, and audited at least annually. This will help keep information from walking out the door.
12. Personnel from Human Resources, Information Security, and Legal need to work closely together to share information and to report incidents to law enforcement for prosecution. Insider attacks are usually not as public as other attacks, and generally criminal charges are not sought. If the company would prosecute, this would send a strong message to insiders. The Justice Department posts recently prosecuted computer cases at www.cybercrime.gov and this site provides a good indication of the damage that an insider is capable of, as well as dollar estimates. In many cases, confidentiality, integrity, and availability are all compromised. Educate employees on how to report inappropriate activity, and implement a "Code of Conduct" anonymous phone report line.
13. Enforce the Backup Standard and the Business Continuity Standard listed in the Information Security Policy. Reliable backups and business continuity plans are necessary in case a disgruntled employee is successful damaging the company's customer records and recovery is necessitated.

Availability of the System
GIAC Enterprises is heavily dependent on its computer network to maintain the viability of its business operations. The speed at which an insurance application can be processed and delivered increases customer satisfaction, and increases the bank deposit date for earning interest on premium funds. Since the implementation of the Electronic Application, GIAC has experienced a workforce reduction from streamlined operations, and an additional expense reduction from the time involved in handling and processing the application. The company cannot sustain an extended outage without suffering a financial consequence.

GIAC workstations and laptops are delivered with a standard CD-ROM drive and a peripheral floppy disk drive. The drives are provided to users to facilitate backup procedures, and to allow files to be exchanged. This illustrates the balance that occurs between convenience and security. A vulnerability exists for malicious code to enter the system and network through this avenue. Users could also load unauthorized software on a machine using these drives. A few workstations on the GIAC network employ the pull philosophy from the SMS server for virus updates instead of the push philosophy, and this is vulnerability. E-mail is the most common way malicious code spreads, and GIAC utilizes e-mail extensively and allows employees to receive external mail from the internet. If malicious code caused a denial of service attack and an outage occurred for an extended period of time, the revenue lost would be substantial, not to mention the cost incurred in clean up activities. The time, money, and resources involved in clean up activities can mount in a hurry on a network the size the GIAC. Malicious code causing a denial of service attack creates a loss of productivity for the associates unable to perform their job functions, which results in increased costs. Associates garner a loss of confidence with the system when viruses occur. As more positions are tied to the use of the Enterprise Application, the severity of an outage will continue to increase. GIAC can also experience a loss of information if the information, and backup copies, are damaged beyond repair. Consequences from the loss of information were discussed in the previous risks identified. The effects of the malicious code will decrease the company's ability to provide prompt customer service during the time of outage, and will tarnish its reputation with customers. Negative publicity can result from a sustained outage caused by malicious code, and customer confidence in the ability of GIAC to mitigate risks will diminish. It is not good for an insurance company to be viewed as an organization unable to mitigate risks. Viruses have become more sophisticated, and therefore can prolong the outage and increase the damage caused. According to Computerworld magazine, the most common entry points include external media, e-mail, web mail, downloads, and unpatched operating systems. (Computerworld, Mathias Thurman) Unsuspecting users can launch attachments or insert CDs with out using a virus scan and infect the network and cause a denial of service attack. Tools are also available on the Internet for unsophisticated users to launch a denial of service attack on a company.

Mitigation Steps

Mitigation efforts will generally focus on prevention, detection, and decreasing recovery time. GIAC has anti-virus software in place across the enterprise, but some additional protections should be implemented.

1. GIAC needs to implement a push update philosophy with all resources, allowing the SMS system to distribute virus signature updates automatically. Servers are currently under this philosophy, however some workstations are still utilizing the pull philosophy. A push philosophy will result in consistent application of updates, and audit records to verify updates occurred. Scans for malicious code should be conducted on firewalls, servers, workstations, laptops, and other information systems.
2. GIAC needs to educate associates on its Enterprise Information Security Policy. Focusing on when to scan for viruses, how to scan for viruses, and what to do when malicious code is found is necessary.
3. GIAC needs to lock down the configuration settings on Outlook, taking into consideration the business needs of the organization. GIAC should require Outlook to be configured to prompt before executing attachments. GIAC must ensure all items enabled in Outlook are turned off by default, and attachment security is set to "High."
4. GIAC must prohibit the use of unapproved and untested software from any source. The company should also educate users on what to watch for on their systems, and how to report abnormal events. Sharing files by floppy disc or CD–ROM should be minimized across the organization.
5. GIAC needs to implement redundancy in its network architecture, and make sure they have implemented fault tolerant configurations.
6. Procedures for using router filters to prevent users from launching DoS attacks should be implemented. Routers should only forward packets with the correct source IP address, and they should not forward directed broadcast traffic. SYN flooding should not be allowed on your system, and patches should be implemented according to change management procedures to avoid these attacks.
7. All unnecessary services on the system must be disabled. This will limit the malicious code's ability to exploit one of these services.
8. Any quota criteria that can be enabled on the operating system should be implemented. This will help limit propagation.
9. GIAC should monitor its system to create and understand a network baseline. It should constantly evaluate the network activity against the baseline to detect anomalies. Implementing programs such as Tripwire to detect changes in network configurations can speed the detection process.
10. System backups need to be regularly scheduled, implemented, monitored, and tested. Backups are critical to speed the recovery process.
11. GIAC needs to implement a business continuity plan for the critical business processes of the organization. Business partners and systems partners will need to develop the continuity plans together. The plans should be documented, reviewed, revised, and tested semi-annually to ensure their viability. People,

processes, and technology will need to be considered. Many areas created continuity plans for Y2K activities, and if these plans have not been kept recent, they could be used as a resource to help jump-start the update process.

12. Procedures should be created and followed for contacting authorities, and the appropriate steps to initiate an investigation.
13. To reduce the threat from e-mail, GIAC Enterprises should implement stringent filtering e-mail software to quarantine attachments suspected of containing a virus. GIAC should also blocks mobile code (Active X, Java Applets) from entering the network, and technology staff should stay abreast of the mobile code arena. Educating employees about the destructive capabilities of attachments can help in prevention.
14. Employees and agents should be restricted by the security policy from downloading from the internet, and only documented business cases should be allowed an exception. Internet activity should be logged and monitored. The company should educate users on the experience with the Code Red virus; to help explain the cost and effort associated with remediation activities once the network is affected.

Evaluate and Develop Security Policy

A security policy is a vital aspect to the risk management program at any company. This sample policy attempts to address several of the vulnerabilities in the risks identified above. It instructs users on securing equipment, avoiding viruses, and protecting passwords. The following policy was obtained from http://www.ruskwig.com/security_policies.htm

I.T. Security Policy

User Responsibilities

These guidelines are intended to help you make the best use of the computer resources at your disposal. You should understand the following.

1. You are individually responsible for protecting the data and information in your hands. *Security is everyone's responsibility.*
2. Recognize which data is sensitive. If you do not know or are not sure, ask.
3. Even though you cannot touch it, information is an asset, sometimes a priceless asset.
4. Use the resources at your disposal only for the benefit of XYZ Ltd.
5. Understand that *you* are accountable for what *you* do on the system.
6. If you observe anything unusual, *tell your supervisor*.

When using the Company's computer systems you should comply with the following guidelines.

DO

7. Do choose a password that would be hard to guess.

8. Do log off before you leave your workstation, if you are working on sensitive information or leaving your workstation for any length of time.
9. Do ask people their business in your area, if they look as though they do not belong there.
10. Do protect equipment from theft and keep it away from food and drinks.
11. Do ensure that all important data is backed up regularly. Liaise with I.T. Services if you require assistance.
12. Do make sure that on every occasion that floppy disks and other media are brought in to the Company that they are checked for viruses by I.T Services before use.
13. Do inform I.T. Services immediately if you think that your workstation may have a virus.

DO NOT

14. Do not write down your password.
15. Do not share or disclose your password.
16. Do not give others the opportunity to look over your shoulder if you are working on something sensitive.
17. Do not use shareware (software downloaded from the Internet or on PC magazine covers).
18. Do not duplicate or copy software.
19. Do not install any software on your machine or alter its configuration, this work may only be undertaken by I.T. Services staff.

Please note the following

Your PC will be audited periodically.
Logins to, and use of the Company's network are monitored and audited.

FAILURE TO COMPLY WITH THE COMPANY'S SECURITY POLICY MAY LEAD TO DISIPLINARY ACTION.

Evaluation

The policy begins by stating the **purpose** of the document is to ensure the best use of the computer resources, and continues to explain what you need to understand about your responsibility. It is clearly stated, understandable, and written in business language. GIAC will want to expand on the purpose in more detail, and will remove the word "should" from its statements. The biggest shortfall is that the purpose does not explain what issue or risk it is meant to address. GIAC needs to clearly explain the risk to the enterprise when users do not act responsibly with company resources. GIAC computers have been stolen because they were not protected appropriately; company secrets have appeared in public; a virus has been introduced to the network from opening e-mail attachments; passwords have been posted on walls near computer screens and prank messages were sent throughout the organization from one of these machines; software downloaded from the internet has overwritten files and caused machine reloads. This is a serious problem for the company and has required time, money, and resources to resolve. Based on these facts, the need for this policy and the

risk it addresses should be communicated to individuals. Users need to understand why this is important to them and to GIAC Enterprises.

The **scope** of the policy is not clearly separated out in the document, and simply applies to "users." The scope of the policy needs to be clearly defined, listing the individuals or areas it is applicable to. Acceptable use for GIAC will need to be broken down into more specific detail. Individuals need to be able to clearly identify themselves as a user, and listing the applicable users should draw a direct line of accountability.

The **policy statements** describe the activities that users should participate in and those that users should not participate in. The statements are very high-level generic statements. GIAC will benefit from adding more detail to several of the statements for clarification. Several of the statements will need to be rewritten to better apply to GIAC's operations. GIAC specific eight character password requirements should be incorporated into the password policy statement. GIAC will want the policy statements to be standards rather than guidelines, and will change the wording to reflect it is a requirement rather than a suggestion.

The policy does not address who maintains **responsibility** for making sure the policy is implemented. This needs to be added to the GIAC policy, and the role of the Security Council in the creation, review, maintenance, and approval of the policy needs to be clearly stated as the owner of the policy. GIAC created a Security Council comprised of representation from functional business areas as well as agent's offices to develop the enterprise security policy. The members are to ensure a business focus is presented that complements an acceptable level of information risk tolerance. The Council chaired by the CSO, reviews proposed and existing policy documents, and raises for discussion any areas of concern as it relates to the current state of the enterprise. The Council discusses areas of concern. The council makes recommendations for policy modification, adoption, or refusal to the CSO, who has the final veto right. Approvals are implemented in the policy.

The specific **actions** stated in the policy statements are very generic, and do not specifically tell users the "when" portion. Users should be instructed to change their passwords every 30 days, and passwords need to be at least eight characters long with upper and lower case letters, a special character, and at least one number. Simply stating that a user needs to choose a hard password is not sufficient for most users. It is too subjective, and many average users will not know whether a password is hard to crack or not. The policy does states that misuse may lead to disciplinary action, so consequences are stated.

The sample policy was a good framework for a beginning, but will need to be changed and elaborated on to fit GIAC Enterprises.

Revise Security Policy

GIAC Security Policy

Policy Area: Acceptable Use
Document Type: Standard
Compliance: Mandatory
Effective Date: 11/02/2002
Owner: Enterprise Security Council

Purpose:
At GIAC, the security of our computer network, assets, and facilities, are taken very seriously. The purpose of this policy is to describe the responsibilities of all associates to protect the company's assets and minimize the misuse of GIAC computer resources, whether by intentional or unintentional means. Protecting company assets includes the physical security aspects, such as checking visitors in and out of the building, using locking cable devices on workstations and laptops, and storing portable devices out of plain sight when traveling, as well as the information security aspects that include creating and using strong passwords, reporting suspicious activity on your workstation, and scanning all attachments received for viruses.

This policy defines misuse of resources as unauthorized access, unauthorized access with the intent to create an opening for future access, and unauthorized modification of information or data.

This policy will minimize confidentiality breaches resulting from inappropriate use, protect the integrity of data required to conduct GIAC's business, and block the exploitation of GIAC's information and information resources to cause availability issues.

This policy is based on the three information security principles of:
Confidentiality-information accessible only to those with a business need to know.
Integrity-keeping information accurate and complete.
Availability-ensuring the appropriate users have access to information resources when performing their job.

Background:
GIAC has a large computer network that collects sensitive customer information, has many access points, and is utilized by 5,000 independent agents and 20,000 employees. With the increase of laptops and mobile computing in our environment and sensitivity and criticality of the data we collect, information security risks have increased. GIAC laptop computers have been stolen because they were not hid in the trunk of cars or locked in the room hotel safe; company underwriting guidelines, which are trade secrets, have appeared in public newspapers; several viruses has been introduced to the network from opening e-mail attachments; prank messages have been sent throughout the network due to poor password procedures; and software downloaded from the internet has overwritten files and caused machine reloads. This is a serious problem for the company and requires time, money, and resources to resolve.

Scope:
This policy covers all internal employees that work at GIAC, agents, agent's staff, external employees, contractors, third party vendors, and interns that have access to or use any information resources of GIAC Enterprises.

User Policy Statements:
Passwords:

1. Users of GIAC information resources will select quality passwords with a minimum length of eight characters which are: a mix of upper and lower case characters, at least one special (*, &, $, etc.) and one numeric character, not found in a dictionary, not identical to the expired password, not sequential numbers or letters, and not based on anything anyone could easily guess (child's name, spouse's name, etc.).
2. Passwords must be used to prevent unauthorized access to computer resources. Password protected screen savers must be configured to activate within 15 minutes of inactivity and invoked (Ctrl + Alt + Del) whenever your workstation is unattended.
3. Passwords must be confidential and protected by users. Passwords must not be displayed, written down, or shared. Passwords must be changed immediately if they are made known to others, or suspected that they have been breached. All users will be required to change their password every 30 days.

Physical Security:

4. Users must display their picture identification badge at all times. All visitors, and employees who forget their badge, must obtain a badge in Security and must sign in upon entry to GIAC facilities and sign out upon departure. Any temporary employee, vendor, or visitor requesting a corporate temporary badge must provide a signed access form from the supervisor of the department they will be working in. These badges will be colored to distinguish them from employee badges. The access form can be obtained from Corporate Security prior to that date.
5. Users, visitors, or vendors who receive badges or other control area devices are required to return them to their immediate management or escort at GIAC upon a change in status. Access must be immediately revoked. All users must question unfamiliar people in the area regarding their business purpose, and must call Corporate Security department to confirm their explanation.
6. Equipment must be protected from theft in the office and while traveling. Users must store laptops out of sight to reduce the risk of theft. While traveling by car the laptop should be placed in the trunk. While in a hotel, the mobile device should be in the hotel safe. Mobile devices, including laptops, must be physically secured to furniture at all times by using the Kennsington cables while at work and the Defcon cables while traveling. Keys for locking the devices should not be left in plain sight. Barcode tags should not be removed from company assets.
7. Lost or stolen equipment must be reported to your first-line management immediately. The "Lost or Stolen Asset" form must be completed, and procedures must be followed to invoke the corporate call tree to protect company

resources. (See Corporate Call Tree procedures in the Computer Incident Standard)

Software:

8. Users must not introduce software into GIAC's environment unless it is licensed or authorized for use by GIAC. Software is considered authorized for use if it is: authorized by the technology department area responsible for the workstation, obtained through the company approved methods, and a license agreement has been signed by GIAC. Only authorized individuals (those pre-approved by the IT security manager) are permitted to download and install new versions/releases, alter configurations, and fixes of software, regardless of whether obtained from the Internet or CDs. Games and Internet Service Providers software is prohibited from GIAC systems.
9. Users must not copy purchased software unless copying is part of the license agreement. (i.e. Users cannot create a copy of Office 2000 to load on a home computer.) Users should contact Corporate Law department to discuss licensing agreements.
10. Users must not open attachments or files obtained from floppy disks and other medium unless scanning for viruses before initial use. Individuals must not knowingly introduce malicious code or perform unauthorized activities on GIAC resources. If a system is suspected of being infected or compromised, GIAC technical staff should be called immediately, and first-line management should be notified.

Data:

11. Users must encrypt all customer data stored on a computer hard drive to prevent unauthorized disclosure and maintain integrity. Customer data should be retained in accordance with GIAC's records retention policy, and handled according to the data classification controls set up GIAC Enterprises. (See the Records Retention Policy and Data Classification Standard)
12. Users must ensure that all customer data stored on their local machine is backed up regularly. Minimally, partial backups should be completed daily and full backups completed weekly. The ADSM backup software is standard on all workstations and laptops, and you can contact your IT workstation support area if you need assistance. Backup files must be stored in the locked storage cabinet located in each area (agent's have a locked computer closet). All backup copies must be properly labeled and retained according to GIAC records retention policy. (See Records Retention Policy)
13. Users must treat data in a manner to prevent unauthorized disclosure and maintain integrity. (i.e. Use encryption when appropriate, limit the information you provide to others to those with a business need to know, place confidential information in sealed interoffice containers, and hold meetings in secure rooms.) Users must not alter or access data for which they have no business purpose, and must immediately report unintentional acts to IT Security management.

Roles and Responsibilities

All employees, agents, agent's staff, external employees, contractors, third party vendors, and interns that have access to or use any information resources of GIAC Enterprises are responsible for knowing and complying with this standard.

IT Administrators:
-Responsible for configuring systems to enforce password strength (length, expiration) when a user's password is created, changed, or input into the system.

-Responsible for implementing products and controls to help prevent unacceptable use by installing firewalls and IDS systems, utilizing SMS to keep an inventory of installed software and conduct audits to detect unauthorized installation, and by monitoring log files for anomalies, and utilizing filtering products to scan and detect viruses.

-Responsible for providing access control solutions for authorized access, removal of accesses, and monitoring of accesses. Systems must be configured to enforce password strength, and logs must be monitored for suspicious activity.

Management:
-Responsible for notifying IT Administrators of changes in access control relationships and approving and reviewing accesses, reporting the theft of resources, and immediately reporting incidents involving company data and company resources.

-Responsible for training employees on this standard and the Information Security Policy and explaining how it applies to their job functions.

Enterprise Security Council
The Enterprise Security Council is responsible for the creation, review, maintenance, and approval of the Policy. GIAC created the Council, composed of representatives from business areas as well as agent's offices, to ensure a business focus is presented that complements an acceptable level of risk tolerance for the enterprise. The Council addresses all security strategy issues for GIAC Enterprises and modifies or creates new enterprise policies.

Action:

All administrators must ensure compliance with this policy by June 1, 2003.

All users must, as stated above:
-Select quality passwords and change them every 30 days.
-Question unfamiliar people or activities occurring in your area, and call Corporate Security to confirm immediately.
-Store all laptops and mobile devices out of sight, and report lost or stolen assets immediately to Corporate IT.
-Report all potential and actual virus infections to IT Security immediately.

-Scan all attachments, CD-ROMs, and diskettes for viruses prior to use and contact IT Security staff and first-line management immediately if a virus is detected.
-Contact Corporate Law to discuss unfamiliar licensing agreements.
-Encrypt all customer data stored on the local hard drive (your D: drive).
-Perform data backup activities daily for partial backups and weekly for full backups.
-Report unintentional access to data and unintentional altering of data to IT Security and first-line management immediately.

Enforcement

Non-compliance with the information security policy will pose a risk to GIAC Enterprises' information and information resources. Violations of this policy will result in disciplinary action, where appropriate. GIAC reserves the right to review, restrict, and access any information on GIAC resources. GIAC has the right to monitor the behavior of employees, agents, agent's staff, external employees, contractors, third party vendors, and interns on GIAC systems.

Develop Security Procedure
Workstation Data Backup Procedure

Purpose
One of the procedures that can be inferred from the Acceptable Use policy is the Workstation Data Backup Procedure. The procedure to backup workstations and laptops is critical to ensure customer information is accessible and recoverable should an incident occur at GIAC.

Scope
The scope of this procedure includes all users who have customer data stored on the hard drive of their laptop or workstation. All users, with customer data on their hard drive, are required to complete the data backup procedures for the equipment in their possession.

Pre-backup Required Administrative Tasks

1. GIAC Enterprises uses the ADSM backup software utility to perform workstation and laptop backups. The user must have authorized access to the backup software to perform the tasks outlined in this procedure.
2. User must have a basic understanding of Windows and the ADSM software utility and the schedules it creates.
3. User must have access to the locked storage cabinet (or locked closet depending on your location) where a copy of the data backup will be stored.
4. User must have authorized access to the Network Storage Manager server software. This will be used to provide confirmation of completed backup. The Network Storage Manager server creates and stores a second copy of the data on a server in the secured Corporate Data Center to ensure data could be recovered if the building where the laptop/workstation and locked storage cabinet resides were destroyed.

Required Actions

1. Partial backups of all workstation/laptop D: drives are run nightly, at 10:00 pm, to make sure that all business activity has ceased for the day. Full backups occur weekly each Friday at 10:00 pm. An individual must load and leave a CD-ROM in the CD drive for the backup to complete successfully.
2. The workstation/laptop user must run a non-scheduled backup if the machine is not or will not be connected to the network at 10:00 pm. The user is allowed to run a non-scheduled backup at any time during the 24-hour day, but all files must be closed and ready for backup. A backup must be completed for each full business day.
3. The workstation/laptop user must label the backup CD-ROM, Partial_01_27_2003 or Full_01_27_2003. The Network Storage Manager server software will label the stored file Userid_Partial_01_27_2003 or Userid_Full_01_27_2003. The CD-ROM must be stored in the locked storage cabinet used for backups or in the agent's locked computer closet.
4. IT Administration is accountable for setting and maintaining the backup schedules, monitoring the performance and availability of the Network Storage Manager server, monitoring the success of the nightly server backups, and notifying the user if a server backup fails and cannot be restarted.
5. IT Help Desk is responsible for performing the data recovery task when requested by the appropriate user. The help desk is responsible for verifying the identity of the caller, and documenting the call in the help desk software product. The help desk is manned 7x 24, and a designated employee is always available to perform the data recovery request. The help desk is responsible for notifying the designated user when the recovery is complete, or if the recovery failed.
6. The workstation/laptop user is responsible for retrieving the CD-ROM copy of the data backup if the server backup copy is unusable for recovery. The copy must be retrieved from the locked backup storage cabinet, and loaded onto the machine. The user is responsible for verifying the success of the workstation recovery, or notifying the IT Help Desk if recovery failed. A copy of the successful workstation recovery file must be uploaded to the Network Storage Manager server if the server copy was unrecoverable. The copy must be labeled according to the naming convention of Recovery_Userid_ Partial_MM_DD_YYYY or Recovery_Userid_Full_MM_DD_YYYY.

Why Perform Backups?

Ensuring the availability and integrity of customer data is critical to the business operations of GIAC and its relationship with its customers. Information must be available to service customers needs when it is required, must be current, and it must be readable by the business so it can be used.

Backup Process

All workstation backups are scheduled to begin nightly at 10:00 pm on all workstations with customer data stored on the D: drive. This timing insures that agents and employees have completed their business activities for the current workday, and the

machine is available for backup. The ADSM Network Storage Manager server software is setup to complete a partial backup every day of the week except Friday on the local D: drive by backing up all files and folders under D:\Data. It is setup to complete a full backup every Friday of the entire local D: Drive. All backups are set to create and send a copy to the Network Storage Manager server and a copy to the CD-ROM loaded in the local machine. The CD-ROM copies are labeled, Partial_MM_DD_YYYY or Full_MM_DD_YYYY. The Network Storage Manager server copy will be labeled, Userid_Partial_DD_MM_YYYY or Userid_Full_DD_MM_YYYY. The ADSM software is configured to verify that the backup process has been completed by the workstation/laptop.

Verification Process

1. Log onto the workstation/laptop.
2. Open the ADSM backup utility program.
3. Select the "Scheduled Backup" tab, and double click.
4. Open the calendar tab.
5. Check for a "Partial_successful" or "Full_successful" status on the correct date of the daily backup.
6. If the status is "Failed", double click on the job and review error report.
7. Open the Network Storage Manager server program. A popup "successful" window should open. Missing popup window indicates backup failure.
8. Insert a new CD-ROM in the drive, and run a non-scheduled backup to complete a new data backup using the ADSM software.
9. When backup completes, remove CD-ROM from drive and label the copy using the standard label naming conventions described above for a partial or full backup. Store the CD in the locked backup storage cabinet.
10. Repeat steps 2-10 again to verify a successful backup.

Auditing

The Corporate Data Center completes a data recovery test each month in compliance with the Business Data Recovery Policy. A log is completed after each monthly test documenting the success of the test. A copy of the log report is sent to the IT Manager and first-line Business Managers regarding all workstations in their unit. If a monthly restore fails, a problem ticket is opened with the IT Help Desk. The problem ticket case number must be indicated on the monthly test log. IT Help Desk will work the ticket until a successful recovery test is completed.

Internal Auditing audits the compliance with the policy regarding the Business Data Recovery process during its semi-annual review of the Corporate Data Center and its semi-annual reviews of functional business areas. Audit findings and recommendations are made to the management of both groups.

References

Computer Crime and Intellectual Property Section – Computer Intrusion Cases. WWW.CYBERCRIME.GOV Home Page. 16 November 2002. <http://www.cybercrime.gov/cccases.html>

Firewalls - FAQ -Investigative Research for Infrastructure Assurance (IRIA). Institute For Security Technology Studies Home Page, Dartmouth College. 16 November 2002 <http://www.ists.dartmouth.edu/IRIA/knowledge_base/firewall_faq.htm>

Grance, Timothy, Marissa Myers, and Marc Stevens. *Guide to Selecting Information Technology Security Products*. National Institute of Standards and Technology, 9 October 2002 <http://csrc.nist.gov/publications/drafts.html>

Pipkin, Donald D. *Information Security: Protecting the Global Enterprise*. New Jersey: Hewlett-Packard Retail Book Publishing, 2000. p. 63.

Reymer, Martin A. *GIAC Enterprises – Data Backup Security Policies and Procedures.* Global Information Assurance Certification. 7 May 2002 <http://www.giac.org/GISO.php>

Security Policies. Ruskwig.Com Home Page. 11 November 2002 <http://www.ruskwig.com/security_policies.htm>

The SANS Security Policy Project. SANS Institute Resources. 11 Nov. 2002 <http://www.sans.org/newlook/resources/policies/policies.htm>

Thurman, Mathias. *Virus Attacks Can Enter Through Many Doors*. Computerworld Home Page. 28 January 2002. 11 November 2002 <http://www.computerworld.com/securitytopics/security/story/0,10801,67720,00.html>

Top 10 most common info security mistakes made by individuals. Human Firewall Council Home Page. 11 November 2001 <http://www.humanfirewall.com/issues.htm#blueprint/.>

Zimmerman, Scott C. *Secure Infrastructure Design*. CERT® Coordination Center, Carnegie Mellon University. 11 November 2002 < http://www.cert.org/archive/pdf/Secure_Infrastructure_Design.pdf>