Global Information Assurance Certification Paper

GIAC Engineering Services Inc.
IT Security Overview

GIAC GISF Certification
Version 1.0

Chris D. Neaves
1-24-2004

Abstract
GIAC Engineering is a fictitious engineering services company based in Texas. The purpose of this paper is to examine several of the IT security issues raised by a basic security audit. It will attempt to illustrate what is currently in place and identify possible solutions as required by the requirements of the GISF practical.

GIAC Engineering Services

GIAC Engineering is a well established Professional Engineering firm providing complete civil, mechanical and electrical engineering services for public and private needs. Examples of work include design services for various highway and bridge projects for public transportation agencies in 13 states (i.e. Texas Department of Transportation), mechanical design of 3 major business center campuses and design of the electrical systems for manufacturing companies ranging from small, one office sites to large multi-acre facilities.

The company is divided into two major organizations: The Mechanical Services Division and The Civil Services Division. Roughly seventy percent of revenue comes from the Mechanical Services Division while the remaining thirty percent is made from the Civil Services Division. Revenues for the company as a whole were $83 million.

GIAC Engineering Services creates revenue by bidding on various major projects established by state transportation agencies, municipalities as well as privately funded jobs. The key to success is to provide the best professional engineering service possible, while keeping projects cost effective to the customer.

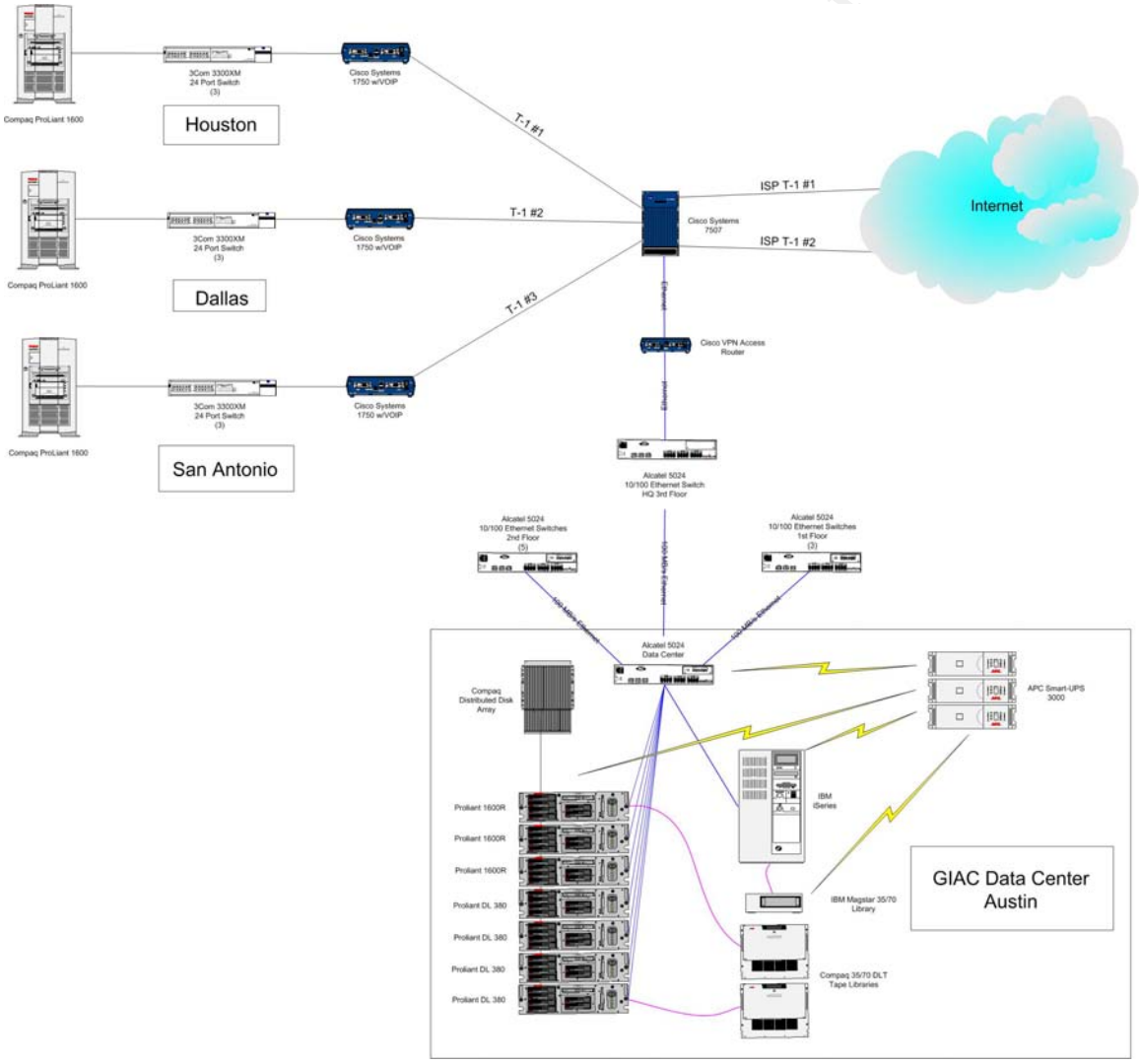
The company is based in 4 locations throughout the State of Texas. The headquarters and IT operations are based in Austin. The other locations are San Antonio, Dallas and Houston. There are 450 full time employees and another 100 part-time staff, which mainly consist of coop students and temp staffing. The geographical breakdown of employees is almost even, with roughly 150 employees at each location.

GIAC Network and Information Service

The IT department provides services that are an integral part of the success of the company. Without storage, design, presentation, communication and collaboration services in which IT provides, a timely and precise product would not be possible. Each WAN location is connected to the headquarters via a T-1. The usage of the private LAN model allows for simplicity, manageability and security. In addition, each location houses at least two servers. One primary server is used for basic file and print services while the other server is used to house the post office for the location. This allows the sites to continue to operate when the ISP or other point of failure interrupts communications. In addition to the WAN sites, the headquarters site houses central servers for storing projects,

contracts, HR services, web services and customer databases. The data center is located on the 2nd floor of the corporate headquarters building. It was originally owned by a bank data center. The floors are raised and the entire room is climate controlled. Taking advantage of the previous owners design, the building also has a small generator to provide emergency power in the case of a loss of public service. The central mail servers are located here as well. These servers route mail to the various post offices and in and out from the Internet.

Simple Network Diagram of GIAC Engineering Services



The company utilizes two separate ISP's to provide Internet service via T-1's. Again, this provides a level of redundancy in the case of communication loss. The main router is a Cisco 7507 while the WAN sites utilize Cisco 1751's. Firewall services are provided using a Cisco PIX 520 and VPN services are

supported with a Cisco 7300 VPN gateway. All sites are 100Mb Ethernet to the workstation employing 3Com and Alcatel 5024 managed switches.

NIS -- Departmental Description

The Network and Information Services (NIS) group is under the direct management of the Information Systems Director (ISD). The mission of this office is to insure that the IT resources of the company are protected and that all IT endeavors are in the best interests of the goals of the company-- to be the best in market.

The main tasks that NIS deals with are:

- New Application Design – Applications that are needed to solve a particular problem. For example, bill payments, travel reimbursements, customer information needs, and / or MIS reports.
- Vulnerability Analysis – Annual vulnerability analysis is performed to insure that all systems are protected to the best level possible.
- IT Security Policy Management – NIS creates and enforces IT policy.
- IT Consultant / 3rd Party Management – Often times, an outside consultant is used to aid in design of new applications, installation of equipment, etc. Before these folks are allowed to work, they must abide by security and access policies (non-disclosure).
- Network Design – When new sites are needed or upgrades are required, NIS does all of the design work for proposal to the CIO.
- Network Firewall Management – NIS also maintains the Cisco PIX firewall where the Internet T-1's come into the company.
- Systems Management – All system maintenance (backups, hardware, software, peripherals) is performed by the NIS group.

The ISD reports directly to the Director of Internal Services. They are responsible for making sure that the services provided by NIS are consistent with the goals of the company. All work up to and including the final design of o project are done on a computer. NIS's main concern is with workflow efficiency. The engineers must have access to workstations that are reliable. They must be able to store their work in a reliable location and the files must remain secure. To get this work done, 15 employees are required in the NIS office.

There are three teams in which NIS can be divided: PC / LAN, Business Systems, and Administrative. Each team and position will be briefly reviewed in order to understand how this group is broken down.

PC / LAN team
Network Analyst – Network Operations / IT Security
Systems Analyst – Server Administration (Windows and Novell)
Microsystems Analyst (4) – PC and application support
Business Systems team

Senior Systems Analyst (2) – Mini Operations and support / Programming
Systems Analyst – Financial Systems / MIS reporting
Programmer Analyst – Applications management
Web Applications Developer (2) – Web presence (Internal and external)

Administrative team
Office Manager – Purchasing and receiving
Computer Support Technician – Helpdesk first line support / management
Student Worker – Misc. needs / PC support

Each employee is issued a laptop to be used in their office as well as when they are on the road supporting customers. NIS provides dial-up and Internet access to network resources via VPN. All users are required to validate into the VPN in order to access anything located on the GIAC LAN.

The ISD creates a budget for the group each year based on projects and estimated needs. The current budget is $1.3 million: $700 thousand for salaries and $600 thousand for travel and capital expenses. When compared to the total revenue of $83, NIS is operating at an efficient 2% of total revenue.

Network Analyst -- Description

Since the company is relatively small in size, it falls under the job of the Network Analyst to perform the IT security duties. This job is an established position that is responsible for network design and troubleshooting. The salary for this position varies with experience. The main focus on hiring this position is the employees networking skills. IT security skills are secondary and are looked upon as a bonus when hiring. Roughly fifty percent of the time is spent on network engineering and fifty percent is on securing the company's IT assets. Though the position is not entry-level on the networking side of things, it is the only position that involves IT security. This position reports directly to the Information Systems Director, as mentioned in a previous section.

The primary responsibility of the position is to maintain efficient operation of the corporate network. This includes the design of networks, purchasing of equipment, troubleshooting of network issues, monitoring network traffic, and being the liaison to the companies two ISP's. In order to measure the success or failure of the network, the Network Analyst must gather several metrics to use in monthly reports to upper management. These reports along with reports created by the helpdesk coordinator help the ISD define the success of failure of network operations.

IT security would be the next major area of responsibility. Specifically, the Network Analyst will maintain a Security Awareness Program for the company. This involves ensuring that all users are educated on basic IT security practices and that they are aware of what is expected of them regarding established

security policies and what they should expect from the company. Also included in the Security Awareness Program is a basic IT security web presence. This website allows employees to download antivirus software licensed by the company, read alerts established by NIS, and have access to the corporate IT security policy. Email alerts are also automated and sent to all employees when NIS needs to make sure that the users are aware of a particular threat (i.e. new worm or virus). Performance in this position is measured by a corporate wide questionnaire sent out each year that allows the users to voice their opinions in all of the internal service organizations of the company, including NIS and specifically the Security Awareness Program.

How Does GIAC Engineering Conduct Business?

When someone decides that they want a new building, road, bridge, or other structure, they must have an engineer aid in the design to ensure that it will work properly when it is built. GIAC Engineering Services must sell the customer on every part of the project. NIS is involved in almost every facet of the sale. Each job is ultimately stored as a file on a server. The contracts between customers and GIAC are stored on a server. The conversations between GIAC and the customer are stored on a server. And finally, customer relations and presentations are stored on a server. Since there may be ten to twenty projects working at any time, the information must be available when project managers, CAD experts, Engineers, managers, and multimedia specialists need it.

As previously mentioned, all WAN sites have servers placed at each location. These servers are used to support file storage. All projects are centrally stored on servers located at the NIS data center in Austin. In addition to the file servers at each location, there is a mail post office that is used to support that location. Mail is routed by a central mail server located in the data center.

For instance, let's take a new project scenario. A project manager will receive an email from the Texas transportation department stating that there is a new project available to view. The managers can then look at the project via the web. Once a project is decided upon, a project team is created and plans are developed based on the needs. The CAD files, contracts and other documents are stored on a central server that is backed up each night. A presentation of the project is worked up and again stored on the main servers. Once awarded, the projects are stored according their project number. The files are kept on the server for a year and then archived to DVD and tape.

In order to protect these critical files, the infrastructure must be solid and dependable. The data center holds over 30 Compaq rack mount servers. Storage is extremely important when dealing with projects of the size and scope involved with engineering design. GIAC uses Compaq array solutions to provide redundant and reliable storage. These arrays allow the ease of adding drives as needed, hot-standby drives, and hot server redundancy. Most of the internal

operations applications such as HR and customer relations are run on the company's IBM iSeries system. This is a good choice of system for these applications due to the iSeries' inherent OS security and the robustness and scalability. The applications will be discussed in a later section.

Critical Applications for Business

There are five applications that are critical for GIAC to function: collaboration tools, HR/FIS, customer relation applications, and Internet Access. The first, and most obvious, are collaboration tools. The ability to communicate is more important than ever. Employees have a need to be in constant contact with manager, co-workers, and customers. Without this communication, the company would fail. Every employee has been given access to email, calendars, and task management tools. Email content is regulated on a basic level by the email section found in the corporate IT policy. On the technical level, there is SPAM and antivirus protection working on the message transfer server that attempts to "sanitize" all email in and out. Access to email from outside the corporate LAN is accomplished by authentication to the VPN. Once in, the employee may access email in a similar manner as he or she would in the office.

The next application that is critical deals with HR and FIS. GIAC houses the HR and financial offices together. On the HR side, confidentiality of an employee's information is extremely important. Access to those applications are monitored very closely to insure nothing is leaked or accessed by those without authorization. A statement of responsibility is read and signed by each employee before they are allowed to sit at any computer. This statement is a general review of rules and security awareness issues that are required by the company. In addition, the highest manager of the department the employee works in will assign the systems required for the job function. Generally, the manager will be the owner of the data (i.e. HR Manager will be the owner of the PeopleSoft system) and will give permission for access. On the financial side, access is extremely limited and guarded as well. Billing information crucial to business operations since income is required to pay expenses such as travel and salaries. For those in the department, the applications are protected by Cisco PIX. Using access lists based on IP address and time, the availability is limited. Access to these systems is forbidden from remote sites outside of the corporate LAN except for a limited group of 5 managers. They can only gain access to the systems via the corporate VPN. Once authenticated to the VPN, they must pass a few other validations before access is granted.

The final critical application is the corporate customer relations database. This database holds critical information on all customers. The information contained in the database includes everything from contact information to billing summaries. This information is the most important to the business since many projects are for the same customer and keeping up with past projects, pricing, quotes, meeting agendas and such reflect in the professionalism the company

projects to its customers. Access to this database is required by all project managers. They are responsible for entering the daily information into the application. In addition, financial services makes inputs into the system by adding payment information such as payment tracking, travel payments, reimbursements, etc. Again, this application is made through the corporate VPN. All applications mentioned in this section require their own local authentication in addition to the VPN.

Internet access is the final component required for making access to these applications from outside the corporate LAN work. As a side note, all users are provided access to the Internet. However, as defined in the firewall, only port 80 is allowed by default. In special cases, requests can be made to allow other ports to be opened for a PC on the LAN. On the incoming side, only access to the VPN server login port is allowed until the user is fully authenticated and port 80 on the public web server side is allowed. Currently, no access is allowed to the LAN unless they have been issued a smartcard. This means only employees of the company can access their respective applications and only those employees who have written permission on file with NIS.

Identify 3 Crown Jewels

Every company has something to protect. In the case of GIAC Engineering Services, the most important "crown jewel" would be the customer database. As mentioned in an earlier section, this database contains basically everything regarding customers. If this information was to be accessed by a competitor, they would be able to gain valuable information as to the product provided by GIAC including pricing structure, customer needs and expectations, design secrets, and customer contact information. This data is stored on the iSeries server which houses several important applications.

One is a java-based web application that was written internally to update the customer profile. These web servers do not store any information themselves. The other application is a terminal emulation into the server itself. The application was developed with security in mind. Again, the user must have the terminal emulator software configured correctly and be given access based on the access list, IP address, and userid and password. From the outside, GIAC relies on the security of the firewall and VPN access. As a best practice, the Network Analyst is tasked with reviewing logs from the VPN and firewall daily to look for anything unusual.

Human Resources performs a very important job and is another of GIAC's crown jewels. Each employee has personal information stored on this system. The types of information maintained by the HR systems are:

- Salary information
- Annual performance evaluations

- Certifications and memberships
- Leave information (including medical reasons)
- Disciplinary actions and investigations
- Awards and bonuses
- Personal contact information

This data in the wrong hands could cause many problems ranging from personal threats to fraud. In this case, GIAC uses PeopleSoft as an Application Service Provider (ASP). All access to HR information is made via the Internet via VPN and SSL to PeopleSoft. With this scenario, much of the security burden is on the ASP as outlined in the contract with PeopleSoft. In order to protect the data, there are multiple levels of authentication. Each user in the HR office has specific duties on the system and must be granted rights to the system by written authorization initially. Once permissions are granted and the user is in the system, all modifications are logged by the ASP and reviewed on a weekly basis by the head of the department or owner of the application (usually the data owner in HR). These logs are archived and backed up for later review if an issue ever arises. In addition to the end user making changes, all major programming changes are logged as well. No one programmer ever has the sole responsibility or ability to make a change on a production system. These again are taken from programming best practices. Another area of HR that should be included is correspondence. When there is a need to write a letter regarding an employee, it should be considered private if it contains personal information. With this in mind, there is a storage area on one of the main file server that is considered secure. Access to this area is limited to the HR office and even to the HR user level if required. This allows the Director of HR to conduct an investigation and store sensitive information so that no others can access the correspondence. Again, all correspondence located in an area considered sensitive must be locked down with a document password as outlined in the document management section of the corporate security policy.

With all of the processes involved, a major crown jewel would be the data center of the company. Without it, none of the processes would be able to be completed in an efficient manner that would allow GIAC to compete with other companies in the field. As was mentioned in an earlier section, the Headquarters building is a former bank building. The data center benefits from this building because of the former banks data center needs. The most beneficial is the power layout for the data center. The entire building is backed up by a generator with 14 hours of fuel on reserve. The emergency power will only run essential services (1 elevator, security / fire suppression, and lighting) for the building as a whole. However, in the data center, the generator will power the entire room with circuits to run the UPS's and monitoring systems and security systems. Physical access to this area is limited to those in NIS with a need. The programmers and administrative personnel do not have direct access to the data center. Access is maintained by the building proctor who will assign scan cards (keys) and take fingerprints for the biometric door access system. After an employee has access

to the room, all of the cabinets are coded and may only be accessed with the 4 digit code. This allows access to only those cabinets that contain hardware the employee should be working with at any given time.

There are two types of contracts that are dealt with in the organization: Contracts for services and contracts for simple procurement. GIAC negotiates several contracts for services that are maintained by various groups. NIS negotiates and maintains the contract with PeopleSoft for support. This contract includes telephone support and a maintenance agreement for software upgrades. Another contract that is primarily an NIS function is with HP. Within the company, there are over 250 high-end workstations. HP and GIAC agree to replace these workstations with the latest equipment every 2 years. Also included with this contract are high-end plotters and printers. Contracts not developed in the NIS group are in the HR group. They maintain contracts with a national temp agency for several office support positions.

Contracts and agreements are generally the responsibly of the division with which the agreement affects. They are loosely maintained and stored in the division's area upon the servers. Only those with written access permissions to that data can access the data on the servers.

Contracts for procurement are managed within each division. These range from office supplies to PC's. The standard specifications are issued to each purchasing agent in the division and they must follow these when making purchases. If there are any needed changes, they must be followed up in writing from NIS. This allows NIS to remain removed from the purchasing business, but maintain a level of standardization of systems attached to the network. All of the specifications are maintained on the corporate Intranet and are updated upon need. Access to the Intranet is limited to the local LAN. Each purchase is tracked and paid for by account and project numbers. Once the purchase has been approved by the Division Head, a voucher is sent to central purchasing located at the Headquarters. Money can then be dispersed by check. Access to the central purchasing system was described previously.

Insider Threat Vector

In this age of hackers, viruses sabotage and terrorists, the most prevalent threat comes from the inside of any business.[1] GIAC is no different. Trust is always going to have its place in the corporate world, but IT security must take all measures available to insure the safety and integrity of the data.

The GIAC customer database was mentioned as one of the company's crown jewels. If the customer database data were to get into the wrong hands, there could be serious damage done to the customer and GIAC. Though the access

[1] "Information Security News: Security experts: Insider threat looms largest" (Messmer)

list is closely monitored, there are ways in which the data could be stolen and taken out of the building by those on the LAN. One method would be to copy the data to tape. Those in NIS with access to the hardware and data could make a copy and take it home. Paper output could be used as well by those with given access. Finally, one of the end users could actually read the information to someone on the phone. This would be a huge risk and take a long time. Since the database is not directly accessible to anyone but the employees who maintain it, other methods are highly unlikely. In this case, the highest risk would be those in NIS. Damage to the database would be very difficult since backups are created each night. There are safeguards to prevent the deletion of data. First, a user must have specific deletion rights, next the deletion must be approved by at least two managers. This prevents deletion by one user. Collusion must occur for deletion to take place for a deceptive purpose. Why would someone be motivated to take this information? There are several answers. One would be sabotage. If someone was trying to undermine the company, obtaining information about it's customers for the competition would be an alternative. Another form of sabotage would be to tell a major customer of questionable business practices that could warrant investigation and damage corporate identity.

Contract agreement information is stored in a central server inside the data center. GIAC has contracts with vendors to save money in operating costs. Because of its complexity, the PeopleSoft agreement is one of the most security sensitive contracts. Outsiders have access to personnel data. When there is a software upgrade to perform, question regarding and module, or a general problem, PeopleSoft may need access to the system. This is provided via modem. The HP contract provides for replacement of all high-end workstations every 2 years and plotters and printers every 3 years. Again, access to corporate hardware is available to those outside of GIAC. Finally, the HR department has a contract with a national temp agency to provide several office support personnel in the GIAC cities. This is a very lucrative contract for GIAC as it saves thousands of dollars a year on employment costs. On the downside, access to corporate systems are open to those outside of GIAC.

Management information is stored on the HR system. Information regarding salary, performance, investigations and awards are stored on the servers of the ASP. Access to this information is made to GIAC via VPN and SSL. However, there is a lot of correspondences used in the daily activity of an HR department. All of the letters and memos used when hiring, firing, promoting, investigating, and awards reside on the datacenter servers. The location of these files are access controlled based on permissions on the statement of responsibility given by the division manager. In addition, most, if not all sensitive material is authored and maintained by the Director of HR.

The final threat vector pertains to the GIAC datacenter. The datacenter is the "heart" of operations for the company. All data and communications come

through the center. IT Security policies regarding data storage and access rights are constantly reviewed and audited for new threats and needed updates. Physical security was briefly mentioned as well. The physical security points enforced are: written permissions for access, proximity card usage with biometric verification, and coded access racks for equipment. While there are many technologies that can be added to maintain the security of the datacenter, there are other threats to the datacenter that are more difficult to defend against. Natural disasters are a real threat in this part of Texas. The most notable threats are flood and tornado. During tornado season, there are usually at least 5 times a tornado touches down with in the county the datacenter is located. If a tornado was to hit the building with enough force, there would be little left to salvage and relocation would be the only alternative. For this reason, offsite backups are crucial to the business strategy of GIAC.

Most of the threat vectors mentioned in this section are permeable to those in the NIS group. This is due to the nature of the job that those in NIS perform. As in most companies, the support organization requires access to those applications in which they provide help. The customer database is available to those analysts that maintain the database and those who maintain the hardware. The motivations to steal or damage the data may stem from competitors looking for an unfair edge to revenge. Access to the contract information can be made by the server manager. Since they have full rights to the servers, they have access to everything. This means access to HR correspondence as well. Data could be stolen or damaged very easily by someone in the server management position without suspicion.

Outsider Threat Vector

Stealing information in order to gain an advantage has been in the business world for thousands of years. In the IT world, things are no different. The customer database used by GIAC is the most important data the company owns. Outsider access to this data threatens the company's future. Access to the information in the database is constantly reviewed and audited. However, authentication is made by userid and password. All employees are asked to make passwords as difficult as possible. However, users always find it difficult to remember passwords and tend to use simple words for passwords. Another obvious violation of the policy to leaving systems logged in when away from the desk. Either by guessing the password or simply sitting down at a system which is already logged in can provide all the access a user needs to steal information. It is for these reasons that access to the database may be accessed by those without rights.

For example, let's take a user that works in a GIAC office who is a graphic artist on a project team. If the artist knows the project manager's userid (which are not difficult to guess at most companies), then they can make up to 5 guesses as to the password. The project manager will get the password reset and the perp can

guess again at a later time without the manager thinking twice most times. The most obvious way to gain access to applications is to have the user with access make the connections. Once the login access is provided, the perp may look at whatever they wish. Many times they can make printouts, write down information, or copy desired information to a media device if allowed. The artist in this case will most likely not be questioned or raise any alerts since they belong in the area. This information could then be removed from the building and reviewed. Since the information contains information that could prove valuable to competitors, the perp may want to cause damage to the company and sell the information. Another way to cause damage would be to give information to the news media in an attempt to damage the company's good will.

Malicious Code Threat Vector

This section will cover how one crown jewel may be violated by introduction of malicious code. In this case, the servers in the data center could be a target. The data center servers run on a variety of server operating systems. Most of the file storage servers are running on Novell's Netware 6.5 and all of the web servers (Internet and Intranet) are running Microsoft's Windows 2000 Server. It is a well documented fact that there are security holes in all operating systems, but because of its desire to be user friendly, Windows is inherently risky.

In this scenario, a user on the local LAN uses a browser to check their personal email account from their ISP. One of the emails, seemingly from a friend, instructs the user to open the attachment to obtain the latest fixes from Microsoft. The user opens the attachment, but nothing appears to happen. However, the attachment runs a program on the user's computer that downloads another program from an Internet site in the background and installs itself. Unknowingly the user just installed a variation of Back Orifice, a Trojan that allows remote access to systems in which are infected. The worm also installed a program that looks for a particular unpatched versions of Windows by using ICMP. Once an unpatched host is discovered, the Nachi variant can set up shop on it and spread further. The Nachi worm exploits the DCOM RPC and WEBDAV vulnerabilities in Windows. With enough hosts infected the LAN would eventually crawl to a halt because of the emense ICMP traffic. This denial of service could prevent critical milestones in projects from being met, backups from working correctly, important correspondence from getting to clients. Any and all of these problems could damage a client's image of the company resulting in loss of projects and income.

In most cases the SPAM filters, if used, will catch such attachments. However, if it is a new variant or newly introduced worm, it could take 1-10 days for a company to come up with the correct filters to catch the bug. The same goes for antivirus vendors. In this case, the user had antivirus software installed on the system, but had disabled it because it "slowed my system down to much." Antivirus software does place some burden on the machine and is often times

disabled. A good alternative would be to install a centrally managed software that can push the product out to the clients and have no easy manner in which to disable, or modify the settings.

Most Severe Threat

After a broad evaluation of the security posture at GIAC Engineering, several issues have been uncovered that could be exploited by numerous threats. However, the most severe threat to the IT resources of GIAC comes from the outside in the form of viruses or other malicious code introduced via email. These programs are commonly known as viruses, worms, or Trojans. They all work by having an attachment executed that attempts to exploit a known vulnerability (as in the Nachi example above). If the vulnerability exists, the exploitation occurs with varying results such as data loss, data damage, denial of service, unnecessary panic to name a few.

The likely occurrence of such a threat appearing is extremely high. Published in December 2003, MessageLabs noted that the ratio of virus-infected emails versus clean emails increased 84% last year.. In 2002, for every 212 emails, there was 1 virus-laden email compared to 33:1 in 2003[2].

As the threat of email attachments carrying malicious payload increases, so does the risk of loss of GIAC data or revenue. For example, many of the bugs over the past year have caused denial of service attacks. When a DOS attack occurs, server files, the Internet, email, etc. are difficult or impossible to use due to the overwhelming amount of traffic on the network. The resulting costs to the company can be very high. Time and labor to get these machines "cleaned" can be very expensive, not to mention the loss of time for possibly hundreds of employees.

In addition to DOS attacks, data corruption or loss can occur. Most of the time, the malicious code is executed by a user. In some cases, the virus will affect not only local files, but network shares or mapped drives. If executed by a user with enough rights (a system administrator or project manager) the results of a data damaging bug can be extensive. All data could be lost that has been added since the last backup in all cases, but could be extensive with the rights these employees possess.

The operative word when referring to this threat is not IF, but WHEN? Given the statistics above, chances are extremely high that a threat of this nature will hit GIAC soon resulting in loss.

[2] MessageLabs, Intelligence Analysis

Remediation Strategy

In order to protect the assets of GIAC Engineering, the most obvious and imminent threats must be addressed before all others.

As detailed in the previous section, the threat of malicious code entering by email is a major concern and must be corrected. GIAC currently uses a PC based anti-virus tool on all workstations. This software is required and provides a good basic layer of protection. In most cases, the PC based software will catch viruses as they are opened on the PC; however, it is ineffective on worms and Trojans. Another shortfall of the PC based solution is the ability of the user to disable the scanning feature.

In order to fully protect GIAC's users, all email must be scanned before it enters the email system. When the mail arrives, it is scanned for malicious code. If code is found, it is stripped off and never introduced into the system. In addition to scanning for viruses, worms, and Trojans, the scanner will also be able to scan the attachments for extension types that can be dangerous. By limiting the available attachment extension types, GIAC can further reduce the risk of introducing malicious code into the system. This list can be managed by NIS. A side benefit of most of the anti-virus scanners, SPAM is also scanned and stripped. This additional benefit will save time and money. As in any security related area of IT, policies will have to be added and adapted to meet the needs of the users.

Implementation of a scanning system should be fairly painless to get up and running. The end user should not be affected with the exception of a brief outage of email when adding the new hardware.

The timeframe for implementation is based on the following items:

- Needs analysis
- Documenting requirements for solution
- Identify top 3 products in class
- Install and test in lab setting
- Make product recommendation
- Purchase product
- Obtain training (if required)
- Install
- Make policy adjustments (as required)

Due to the importance of getting the protection this solution provides, the timeline should be escalated. In this case the product should be in place no longer than 1.5 months from now. This should provide enough time for sufficient research to be performed and decisions to be made.

Due to the nature of the project, the management of the system should fall under the Systems Analyst. Since the duties of the Systems Analyst include email administration, the email anti-virus / SPAM server should be added to the duties list. Actual administration of the server will not add considerable time to their day. Most work on the server will only include normal server maintenance and occasional tech support in the event there is a problem with the scanning software or hardware.

The new scanning system will require new hardware for the software to reside. This new server will be a standard hardware selection with appropriate redundancy as used with all servers. The server will reside in the DMZ of the firewall and will scan all SMTP mail both incoming and outgoing. Incoming for obvious reasons and outgoing so that GIAC does not spread any virus in the rare case something gets in. This could be extremely bad for GIAC's image to send a virus. Scanning outbound is an act of due diligence.

Once the email is scanned, it is routed to the email system and distributed to the appropriate post office and user. In the event that malicious code or a "banned" extension type is found, it is stripped off and a notification is sent to both the sender and recipient as to why action was taken.

As with any software implementation, the initial cost is small compared to the ongoing costs associated with maintenance. The budget for this project for the first year is approximately $14,000. This is still a small cost when compared even a single incident that requires action to clean and restore data to its original state. The following breaks the costs down.

- Scanning software = $5,000
- New server hardware = $5,000
- Training = $1000
- Analyst time = $3,000

Since the software is dynamic and constantly requires anti-virus and SPAM signature updates, there is a yearly maintenance fee. The fee per year is $4,000 and is renewed based on purchase date.

Finally, the ability to block SPAM (unsolicited email) can prevent the hundreds of scams that are incurred by email. If the user is not receiving SPAM, they are spending their time more efficiently at work and not subjected to the barrage of junk mail which is wasting time and storage resources. Gartner Group has projected that over 50% of business email is SPAM.[3]

[3] Messaging Architects, GW Guardian AV+ Product Literature

Backup Strategy

GIAC has an existing corporate backup strategy. However, it is clear that the company policy of only storing data on networked storage is not being realized. When discussed, the users often give the following reasons why they do not follow procedure and store corporate data on the servers and keep it on the local drives of their systems:

- Unreliability of the network
- Portability
- Ease of Use
- Default locations in software

At times, the users claim that they cannot access the network drives or receive an error when saving, so they just keep the data on their system until later. Habit forms and they continue to store data on the local drive. That is, until their system fails and a lot of hard work is lost.

When portability is claimed, the user is often reminded that GIAC has VPN access to the servers and applications. They sometimes take the time to get the VPN access working again, but often times maintain old ways.

Ease of use is a quick way to claim laziness or disregard for policies. Reminders of the policy to store files on the network drives are given in all cases, but often fall on deaf ears.

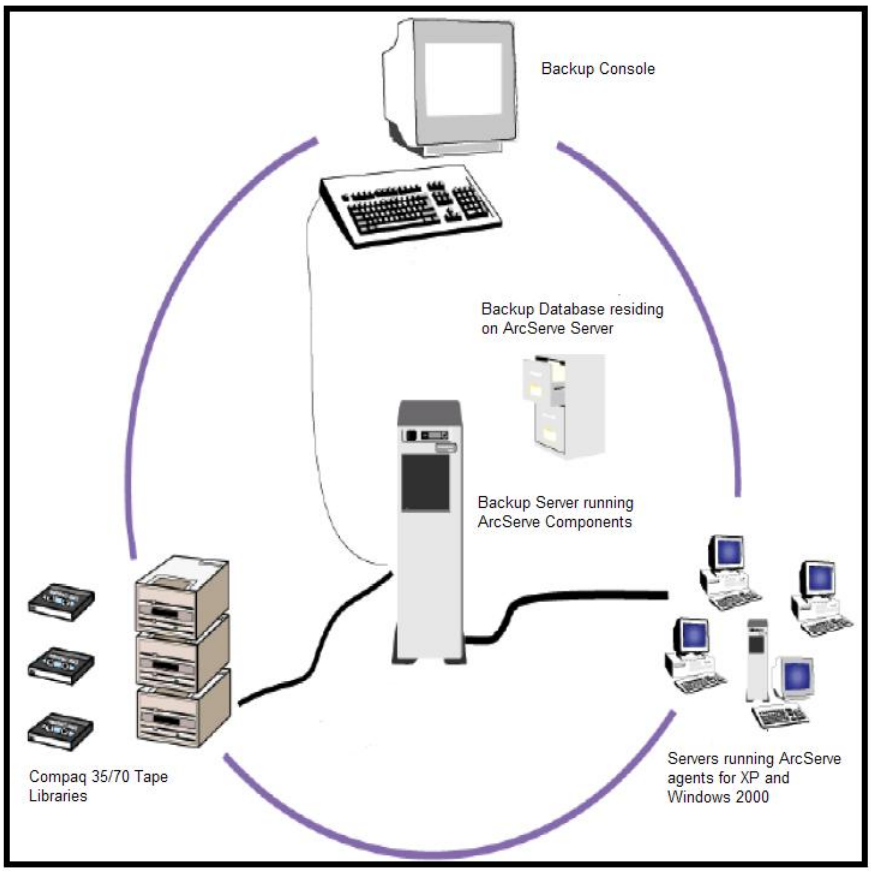
Many times, when software is reinstalled, the default locations for saving information is set to local drives. Users are instructed and tutored on how to change these settings.

Regardless of the excuses, there are users not following policy. The following section will attempt to create a backup plan for the NIS group that will provide backups of local systems while providing a foundation to migrate the plan to encompass the entire company at a later date.

Most, if not all users in the NIS group follow the procedure to backup all data to the network drives. However, for this plan, all systems local drives will be included in a monthly backup plan. The plan is simple, once per month, data from the users workstations will be backed up and archived to tape along with the datacenter's servers.

In order to achieve this, some software will be required on all workstations. The datacenter uses Computer Associates ArcServe version 9. One backup server services the Netware servers while the other services the Windows servers. The two backup servers are each attached to an HP 35/70 DLT library.

All of the NIS workstations are running Windows XP Professional on Dell Inspiron 8500 notebooks. The ArcServe backup agent for XP is included in the price of ArcServe when purchased as an Enterprise version. Once installed on the workstation, the server administrator (analyst tasked with backup duties) will connect to each workstation to setup the job. The job consists of what will be backed up, when, and where to place the data. In this case, the entire hard drive shall be backed up at 9am on the last Friday of the month and will be placed on the appropriate tape group for that day in the regular rotation. If the machine happens to not be on at that time, the job will retry for that workstation until successful and place it on the next tape group. The following diagram illustrates how it works.



Implementing and maintaining this plan is extremely cost-effective. As mentioned previously, the software is already included in the corporate wide solution. The only additional costs will be the time it takes to install on each workstation (~10 minutes) and configuration of each job (~15 minutes). Total time required to implement would be less that 1 day for two analysts. Given the amount of data, there may be an additional cost for media. This is estimated at 24 tapes. Total annual cost for the project is roughly $2,000. One huge advantage would be that the data would be able to rotate in GIAC's offsite rotation, which will be discussed in the next section.

Offsite Backups

Backups are the only thing a company has in order to recover from data loss, either natural or man-made. Keeping all of the supplemental backups in house is a huge mistake, but often overlooked when planning backup procedures. Since GIAC is a smaller company, a companywide plan will be put into place for offsite backups. The following plan will allow sufficient rotation of all of GIAC's data to an offsite location.

GIAC Engineering maintains 10 file servers and 2 web servers that are backed-up on a regular basis. The file servers are running Novell Netware 6.5 and the web servers are running Windows 2000. Selected volumes and folders of the servers are backed-up on a daily and monthly basis. Please see the table below for list of all backed-up servers.

Server	OS	Contact	Media
GIACSRV1	Netware 6.5	Systems Analyst	Compaq MSL 5026 Library / Datacenter
GIACSRV2	Netware 6.5	Systems Analyst	Datacenter
GIACSRV3	Netware 6.5	Systems Analyst	Datacener
GIACSRV4	Netware 6.5	Systems Analyst	Datacenter
GIACSA	Netware 6.5	Joe Person	Compaq 20/40 DAT / San Antonio
GIACDAL	Netware 6.5	Steve Person	Compaq 20/40 DAT / Dallas
GIACHOU	Netware 6.5	Charles Person	Compaq 20/40 DAT / Houston
GIACNIS	Netware 6.5	Systems Analyst	Datacenter
GIAC2K1	Windows 2000	Systems Analyst	Compaq 35/70 DLT Library / Datacenter
GIACBRIO	Windows 2000	Systems Analyst	Datacenter
GIACAPPS	Windows 2000	Systems Analyst	Datacenter
GIACTEST	Windows 2000	Systems Analyst	Datacenter

Server Types

The file-servers are divided into 2 categories: local servers and remote servers:

Local servers comprised of servers that are physically located within the Austin Datacenter. Remote servers are located outside of datacenter. Server locations are noted in the media column.

Daily Backup Job

All daily backup jobs are run every weeknight at 7:00 PM, Monday-Friday. Each morning the designated person changes the daily tape on the tape drive to enforce one-week rotation of backup except for those servers which are attached or backed up by a tape library (automated changer). All of the servers use one tape per backup job with the exception of GIACSRV1 which requires 2 tapes. This is due to the amount of the data being backed-up each night and the combination of tape drive capacity (35/70GB). With exception of the two backup controlling servers, which are physically connected to the libraries, the backups are made remotely by using backup agents (small programs installed on each server) on each server.

Rotation and Storage

To ensure data integrity in the case of disaster, there are 2 sets of Wednesday tapes from each local server that are being rotated every week. Wednesday's tapes from all local servers are taken off-site every Thursday morning. The contact person from each site will unload the tape and place it in overnight mail to be sent off to either San Antonio for the data center's tapes and to the datacenter's systems analyst for the WAN tapes. The tape will then be kept at those respective locations for approximately 1week until they are returned to the original location and loaded to the tape drive for another Wednesday's backup job. The data center's Wednesday's tapes are kept in a secure drawer in a server closet room in GIAC's San Antonio office. Joe Person is in charge of the box and those tapes. The systems analyst keeps the other servers' Wednesday's tapes and all servers monthly tapes in a fireproof safe in the data center.

Monthly Backup Job

In addition to the daily backup, monthly backups are also run on all local and remote servers. These monthly backup tapes are stored and never replaced for archive purposes for a period of one year. After a year period, these tapes are then reused for regular daily backup jobs. The monthly backup jobs are run on the last-working day of each month. The systems analyst coordinates the retrieval of these tapes from all sites. The first morning of each month the validity of the backup job that ran the night before will be checked to make sure the tapes sent contain valid data. If the backup job failed on the last day of each month, the previous successful backup tape will be used instead. The designated person from each site will send the last working day of each month backup tape to the systems analyst to be stored. They will then send a blank tape to replace the tape used for monthly backup. In the case of remote offices, NIS will send 12

blank tapes and the shipping packages to each site to replace and to send the monthly tapes.

Annual Tape Archive

NIS keeps a yearly backup tape for each server. The August monthly tapes from each server are kept for archive purposes. These tapes will never be reused and are stored permanently in the data center.

Windows 2000 Server backup

All Windows 2000 server backups are run from the GIAC2K1 server. GIAC2K1 hosts the backup server that is attached to a 35/70 DLT Library drive. All Windows servers, as noted in the chart, run backup agents on each machine which allows GIAC2K1 to access data on the agent servers.

Business Continuity Planning

When building a business continuity plan, there are two important tasks that must be completed in order to insure the BCP will work. The first task is to conduct a risk assessment of the company. The risk assessment deals with identifying GIAC's greatest risks. Examples of this would be:

- Power Outages
- Fire
- Flooding
- Disgruntled Employees
- Vandalism
- Bomb Threat
- Earthquake

The second task is to conduct a Business Impact Analysis (BIA). The BIA will determine:

- The length of time without providing service before losing revenue.
- The cost to GIAC resulting from loss of service.
- The cost of lost productivity due to an event.

Both of these tasks together will allow a measure of the critical systems to be restored in the case of a disaster. The following is a basic design of a BCP that GIAC can follow to get IT services back up and running in the event of a disaster.[4]

[4] "Business Unit Recovery Planning" (Wills)

Scope

The administrative plan for recovery from a disaster at the GIAC Network Operations Center (NOC) is designed to be a working document containing procedures and information needed to recover lost computing capability. This possibility is particularly worrisome because of the center's dependence on services beyond GIAC control, such as power, telecommunications, and ISP networks. The threats of greatest concern are fire, electric failure and malicious mischief. Since restoration of services to clients in such situations would be technically complicated, the need for preplanning recovery action is important. Basically, the plan is to move critical functions to the alternate site and run them there until service is restored at the GIAC data center.

Organization

The plan is organized into five sections and each section deals with particular problems likely to exist in a disaster situation. The nature of these problems suggests that plans for recovery address each step individually.

Assess damage.

- Assemble the disaster recovery team, assess the extent of damage, define the situation, and determine what hardware, software and human resources are available.

- Alert GIAC Administrators, the Director and the Network Availability Center that a problem exists, and the need for re-establishing the network to an alternate site.

- Determine the best alternate site based on the situation assessment, and an estimate of how long resumption of normal operations will take. Notify the selected alternate site of the situation.

- Contact hardware vendors and provide list of required hardware/equipment as soon as possible. Request that emergency order be expedited.

Move to Alternate Site.

- Move all necessary equipment and backup data. Recover all usable hardware, including Uninterruptable Power Supplies (UPS's) and network hardware. Retrieve backup tapes from off-site storage, if needed. Purchase any required items from local economy using emergency purchase procedures. For example, contact local PC vendors to determine immediate availability of a

PC that could be configured as an interim server. Contact TAMU departments and other TAMUS agencies for the possibility of loaner equipment--UPSs, network cards, PCs, servers, etc. Prepare the recovery site for operations and install necessary hardware, software, and telecommunications.

Operate at Recovery Site.

- Schedule personnel work shifts and equipment installation. Establish a processing schedule of critical systems.

Return to Normal Operations.

- Complete repairs to original GIAC computer site and replace all damaged equipment. Repairs to the original site would be started at the same time as the move to the recovery site. When repairs are completed, move normal operations to original site, and then remove the installed GIAC and hardware software from the backup site.

Each of these sections is treated in the plan as a set of assignments for areas of responsibility of the Computer Disaster Recovery Team. The designated areas of responsibility are as follows:

- Coordinator: Information Systems Director
- Center Operations: designated by Coordinator
- AS/400 restoration: AS/400 System Administrator
- Network restoration: Network Systems Analyst

Distribution

The Information Systems Director determines the distribution of this plan and the number of copies. There will be two copies of the plan in the off-site storage area, one in the GIAC data center, as well as others.

Testing

The disaster recovery plan should be tested no less than on an annual basis.[5] To test the plan, a disaster will be simulated and the disaster team will run through the procedures to make sure everything will work. The test will include recovering the off-site backups and walking through a simulated restore

[5] "BCP Testing Techniques and Alternatives" (Williams and Keehan)

procedure. The particulars of each test, results, and any modifications to the plan will be documented.

Scalability

This simple approach to a BCP can be scaled for a single site or for the entire company. Details will need to be worked out as to exact relocation sites. Most vendors make having standby servers, generators, network equipment purchased before an event a thing of the past. With a list of vendors and equipment in the BCP document, procuring all required systems will be done in a timely manner.

References

Messmer, Ellen. " Security experts: Insider threat looms largest". 12 December 2003. URL: http://www.nwfusion.com/news/2003/1208infowar.html (16 January 2004).

MessageLabs, Inc. "Spam and Viruses Hit All Time Highs in 2003". 8 December 2003. URL: http://www.messagelabs.com/news/virusnews/detail/default.asp?contentItemId=613&region=america (24 Jan. 2004).

The Messaging Architects, Inc. "GW Guardian AV+: The best anti-spam and anti-virus solution". Product Documentation. URL: http://www.gwtools.com/sales/pdf/gwguardian_suite.pdf (24 Jan. 2004).

Wills, Jim. "Business Unit Recovery" CONSEC '01 Security Conference. Texas Department of Information Resources, Austin. 24 Sept. 2001

Williams, Kelly and Keehan, Meg. " BCP Testing Techniques and Alternatives". March 2002. URL: http://www.contingencyplanning.com/PastIssues/Mar2002/6.asp (14 January 2004).

Last Updated: July 25th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Portland SEC301	Portland, OR	Sep 18, 2017 - Sep 22, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Cupertino SEC301	Cupertino, CA	Oct 02, 2017 - Oct 06, 2017	Community SANS
Community SANS Toronto SEC301	Toronto, ON	Oct 02, 2017 - Oct 06, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Boston SEC301	Boston, MA	Nov 06, 2017 - Nov 11, 2017	Community SANS
Communtiy SANS Chantilly SEC301	Chantilly, VA	Nov 13, 2017 - Nov 17, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Houston SEC301	Houston, TX	Dec 04, 2017 - Dec 08, 2017	Community SANS
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced