INFORMATION SECURITY FUNDAMENTALS+

GIAC ENTERPRISES

SECURING OUR CUSTOMERS' FINANCIAL TRUST

GISF+ PRACTICAL ASSIGNMENT

SUBMITTED BY BARBARA SLAGEL
DATE: SEPTEMBER 20, 2004

GIAC Enterprises

SECURING OUR CUSTOMERS' FINANCIAL TRUST

SUMMARY

GIAC Enterprises has hired a Project Manager with significant duties in security administration and planning. This paper outlines key issues for GIAC including business drivers, critical systems and functions, and methods for protection and restoration of vital information. The Project Manager must address these issues in response to requests from her supervisor. Many recommendations for improvements to GIAC Enterprises are included.

DESCRIPTION OF GIAC ENTERPRISES

GIAC Enterprises is a small, not-for-profit Trust Company. We specialize in handling the assets of individuals and businesses of medium to large net worth. The primary source of revenue are the fees that are charged on the accounts that we maintain. The company earns about $1.5 M in revenues each year.

The IT organization contributes to revenue generation by providing the services required to maintain and service client accounts. A purchased software package, Series 7, is used to gather client information and manage accounts. A relationship with an external vendor provides us with current account valuations on a daily basis.

GIAC Enterprises is located in northern Indiana, and no satellite offices exist. Customer service representatives travel to provide needed one-on-one contact with clients. There are 11 full-time employees. Key positions and salary ranges include:

- President and CEO ($125,000 - $150,000 per year)
- CFO and Controller ($98,000 - $110,000 per year)
- IT Director ($70,000 - $82,000 per year)
- Operations Manager ($63,000 - $70,000 per year)
- Customer Service Manager ($68,000 - $73,000 per year)

Complete payroll load is approximately $750,000 (not including benefits).

IT INFRASTRUCTURE AND DIAGRAM

The following diagram details the technical infrastructure of GIAC enterprises. The main software used for gathering client information and managing accounts is on a Windows server in the internal network. Many workstations are connected to the network and server within the network. User access is controlled through user ID and application controls.

Data to be presented on the website is pushed out to Network 2 through the data transfer firewall. The web application in use is on the web server which is in the demilitarized zone. The web application makes request for data inside network 2 and then network 2 sends the information out to the web server. This provides protection for the production system inside the internal network. Firewalls are placed to prevent unauthorized access or attacks on the systems, and the internal network is highly protected. VPN connections are made through the internal network firewall.

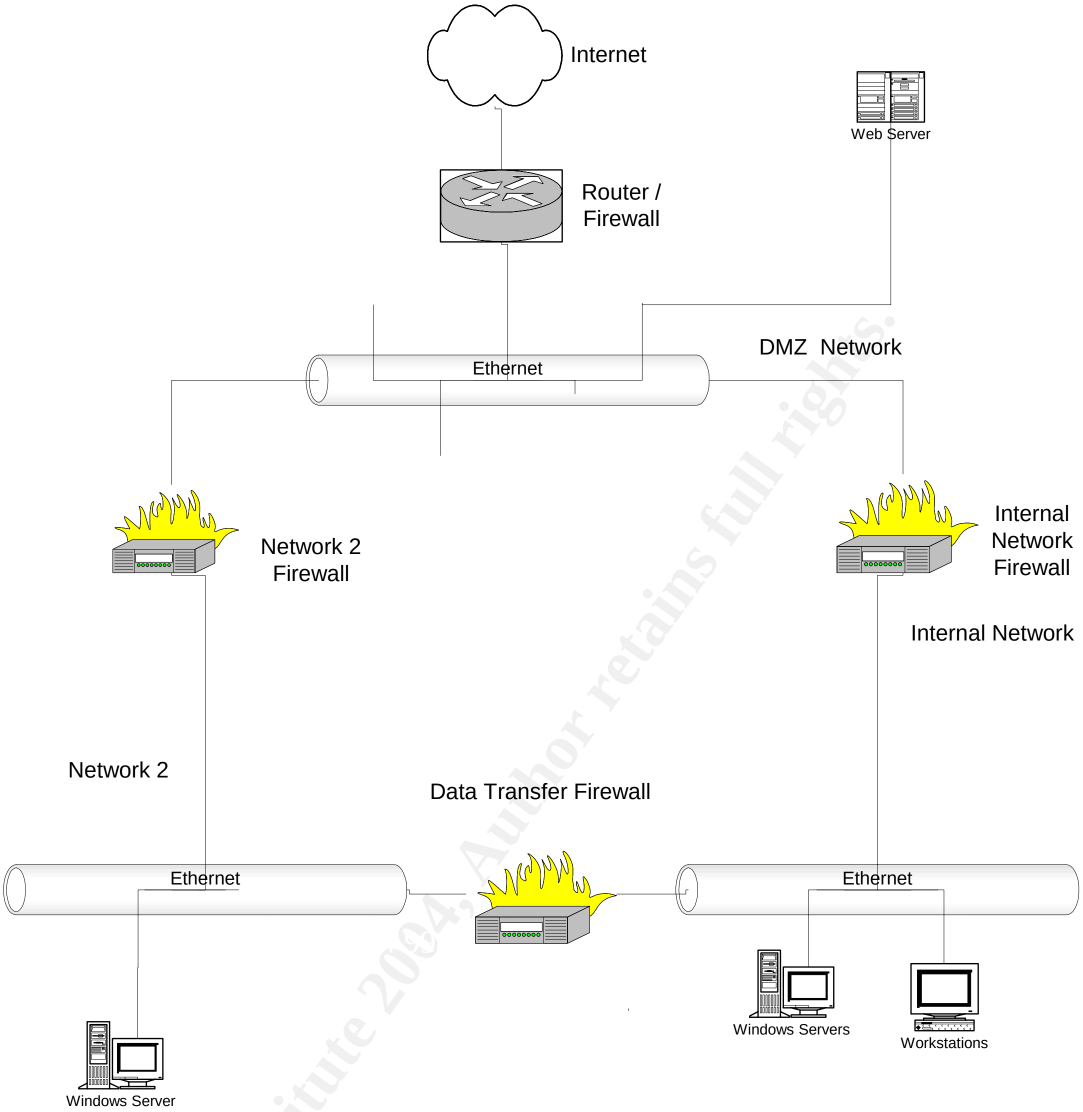
Several mechanisms are in place to protect computers located on the DMZ and Internal Network from intrusions. For the DMZ, filtering rules are in place on the router that connects the DMZ to the Internet to prevent IP address spoofing and port scanning. In addition, server hardening measures and IP filtering rules have been implemented to the server from the Internet and to control the types of network traffic allowed between the web server and Network2.[1]

All email is sent through a vendor, Postini, which strips out emails which are potentially spam and virus contaminated. Then the email is routed to our email gateway through the DMZ. The gateway is located within our internal network. At the gateway, further virus scanning and blocking rules are set up. Then email is delivered to the users' mailboxes.

Firewalls are used to separate the three network segments from each other. The firewalls limit the network traffic that can find its way into the secure network from the public Internet.

Please see the network diagram on the following page for additional detail.

[1] Plank, Richard. "Technical Risk Analysis." Company Confidential Publication. July 13, 2004.



DESCRIPTION OF INFORMATION TECHNOLOGY OFFICE

The information technology office mission is to use our resources to consistently deliver value to the business area to enable the organization to attain its mission: To serve Our Customers with Trust. The IT Director heads up the office and reports directly to the CEO.

Our office is responsible to ensure that IT dollars are spent wisely, so that there is a return to the business for every IT investment. In general, the IT shop enables the company to actually conduct business by providing technology services and software contact clients, maintain client information and maintain account information. The executive management team meets monthly to review potential IT projects and ranks them based on current business need. When possible, an ROI is estimated for the project.

Once a technology project is approved, IT personnel work directly with the users affected by the project. Generally a project team is formed, and they report progress regularly to executive management.

Purchase decisions are made jointly with the IT department. Given the direction of the executive team, each project assesses technology needs and makes recommendation to the IT Director for purchase. All technology purchases must be approved by the IT Director.

All IT assets are the direct responsibility of the IT department. This includes workstations, laptops, servers, firewalls, routers, and telephony.

Roles in the IT Department are:

- Network Specialist – responsible for implementation of network design, troubleshooting, and implementing security measures.
- Programmer/Analyst – responsible for gathering business requirements and for system design when needed.
- Project Manager – responsible for leading all projects, securing resources for projects and assisting with capital budgeting and purchasing. The project manager is also responsible for the security program, developing policies and assisting the network specialist and programmer/analyst in compliance.
- IT Director – responsible for oversight of all IT functions.

The IT budget is generally about $150,000 per year. Training is important in our small team since each employee must cover a wide area of responsibility, so about 1/3 of the budget is spent on training. The remainder of the budget is spent on hardware, software licenses, and occasionally, when a large project requires it, consulting services.

JOB DESCRIPTION

My formal job title is Project Manager. However, responsibilities are very broad in our small department. Therefore, I also function as a security and risk manager. Current salary is $43,000 per year (not including benefits). The Project Manager reports to the IT Director.

The primary responsibility of the project manager is to ensure that customers' information is kept private, secure and confidential. Success is based on two factors: (a) no more than 12 security incidents per year with incident handling completed within 48 hours, and (b) appropriate security policies and procedures are in place for regulatory audits.

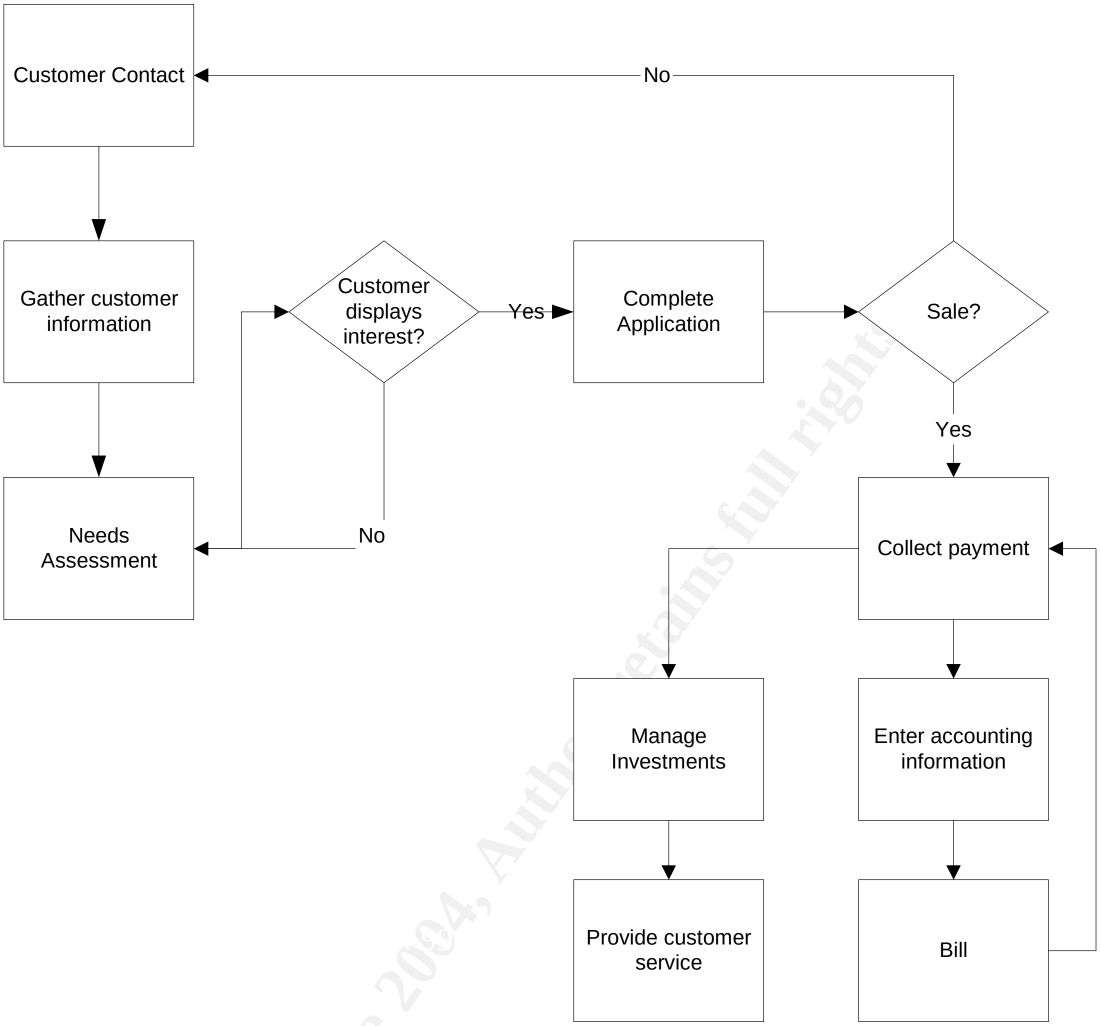
The secondary responsibility is to lead technology projects. Project success is based on the three measures for all projects: time, cost, and scope. These three measures are prioritized for each project, and are weighted for final measurement of the project's overall success. In general, our small department requires that the project manager performs business analyst tasks as well as software evaluation, testing and security audits.

Finally, the job requires that the Project Manager works with all other IT personnel to educate them regarding security issues and provide general awareness for the company.

HOW GIAC CONDUCTS BUSINESS

GIAC is a heavily customer focused business. All business is generated from one-to-one contacts with customers. It is crucial that customer service and sales representatives have all the information that need to provide customers with what they need. Furthermore, it is essential that all back office functions proceed smoothly to enable good service when needed.

The simple schematic on the following page shows the basic processes, at a very high level, that GIAC uses to conduct its business.



Customer contact is generally made in person or on the telephone. However, email is used occasionally, if the customer wishes. We make a concerted effort not to send confidential or personal information via email.

Once the customer contact is made, the sales representative gathers customer information, such as demographics. This process is usually intertwined with the needs assessment. As needs are assessed, more customer information is available and is recorded. Once the customer needs assessment is completed, the sales representative inquires whether the customer is interested in what GIAC has to offer. If so, the process continues. If not, the sales representative will continue to assess needs as long as the customer is willing. This process will likely take multiple contacts.

When the customer is ready to purchase our services, an application is completed for the product the customer wishes to acquire. After the application is completed and more information given to the customer, such as premium or interest, then the sale is finalized. If the sale is not finalized, then the process begins again.

Following the agreement to purchase, the customer will make initial payment for the service. The payment will be sent to accounting for processing and the investment information will be entered into a Investment Management system. The accounting system sets up the process for regular billing, if required (some products are a one-time cost).

APPLICATIONS AND ACCESS NEEDED TO CARRY OUT BUSINESS OPERATIONS

GIAC uses a Sales Force Automation (SFA) tool to capture customer contact information, to perform needs assessment, to keep contact notes, and to complete customer applications. The SFA software is a web-based tool that requires a high level of security. Many of our customers are high net worth individuals and it is important to safe guard their personal information. Sales representatives are able to access the system through the internet, using a secure login.. The system application is located on the web server. The SFA database is located on network 2, and information is sent to and retrieved from the database when needed.

Customer service is provided from the investment management system after the sale. Customer service representatives have access to both the Investment Management system and the SFA system. Contact information is updated in the SFA system, and the investment system is used to explain benefits and make changes to fund allocations. Representatives access our internal network via a dial-up server inside the firewall. They can then use the infrastructure to browse out on the internet, or access applications within the network.

The Investment System is located on the internal network and no outside access is granted at this time. We are considering installation of a web-based customer service module that will allow representatives to change investment information via the web, or allow customers to directly change their own investment information, but given the high need to protect our customer information, we are taking considerable time before implementation to ensure security.

Currently, some basic investment information is duplicated from the Investment System and copied into the SFA database on network 2. This allows the representatives to handle the majority of customer service requests.

An accounting system handles the exchange of funds and rebilling of the customer, if needed. The accounting functions are generally considered to be back-office functions, though customers do receive billings from the accounting office.

Our website is content oriented since our products require interpersonal interaction. Our main concern with the website is that it is not a tunnel into our internal networks. Our email server is on Network 2. Interaction with our vendor for pricing investments is conducted via VPN to our internal network. Internal users access the internet for research and stock price quotes.

GIAC'S "CROWN JEWELS"

GIAC Enterprises is a service organization and therefore its information about its customers and products are essential to GIAC's on-going survival. Without our customer database and Investment System software, we would cease to function. Therefore, we must protect these critical assets. In addition, GIAC must safeguard their customer's personal information to protect our reputation as a safe place to conduct business. Our reputation is vital to our high net worth customers' trust in us.

Customer and Product Information: Customer information is stored in the SFA System, as described in the section above. Because of our small size, almost all employees can access the system, with the exception of accounting personnel. We function on a need to know basis, and since accounting personnel do not provide service to customers, they do not need access to the system. The information is stored in a database located on Network 2. User access is controlled by access to the operating system and application user access controls built into the purchased software. All users can update customer information.

Product Information is stored in the Investment System and is located in the Internal Network. Access is controlled through operating system accounts and application user access controls. The information contained in this system is our most highly prized information. If it is comprised in any way, our reputation as a Trust company is at stake, and it would be highly likely that we would cease to be able to conduct business.

Company Contracts: Company contracts with our vendors are kept in two places. First, the CEO's administrative assistant is responsible to maintain a locked file with paper copies of the contracts. Additionally, outside legal counsel receives copies on contracts for which they were engaged in contract review. The administrative assistant has a MS Access application which identifies key points in each contract and the location(s) of the paper copies. The MS Access application resides on the Internal Network and access to this information is restricted to management.

Management Information: Management information (including salary, bonuses, career paths and current level, performance, background investigations, and educational awards) are on a purchased system developed by our payroll vendor. The application and databases are on the Internal network. Payroll information is sent to the vendor via an FTP website provided by the vendor. Information on this system can only be accessed by the CEO, the CFO and the HR administrator (who actually runs the system on a daily basis).

Reputation: As noted in the section above which describes customer and product information, without our reputation as a Trust company, we would not be able to continue to exist. Our customers are trusting us with their wealth, and the future of their wealth for their families. If our system becomes compromised, or if we have an unscrupulous employee – even one negative experience could have a devastating effect – we will have suffered irreparable damage to our reputation. Therefore, we consider guarding our customers' product information as key to our long-term success as a business.

INSIDER THREAT VECTORS FOR CROWN JEWELS

There are a number of types of disasters that could threaten our company's crown jewels. There are natural disasters, human threats (both internal and external) and technical threats. We have evaluated a number of possible threats and have chosen the following as real threats for GIAC Enterprises.[2]

Natural threats for our organization include:

- Fire
- Snow and ice storms
- Tornado
- Electrical storms (thunderstorms)
- Wind damage

Human threats include:

- Malicious destruction of computers, servers and/or wiring closets
- Vandalism
- Theft
- Employee sabotage
- Unauthorized access

[2] Small, Bob. "Engineering Secure Systems Using Threat Modeling." April 2004. Software Productivity Consortium NFP, Inc. URL: http://www.software.org/pub/externalpapers/sstc2004_small2.pdf (September 20, 2004).

Technical threats include:

- Computer system malfunction
- Telephone line (T1 lines) outage
- Wireless access
- Power failure

A critical consideration for our company is whether employees may have access to information that they should not be able to see. Each of our crown jewels should be protected from unauthorized access. However, in our small company, with most employees filling multiple roles, it can be difficult to assess who should have what information. Additionally, since we are so small, it can be difficult to justify why a person should **not** have access and have them realize it is not a personal lack of trust, but a company policy implemented to avoid potential of problems as the company grows. General access practices are as detailed below:

Customer and Product Information: Customer service personnel and sales representatives may have access to this information. Administrative and accounting personnel may not.

Company Contracts: Administrative personnel (including CEO and CFO) may have access to this information, but all other employees may not.

Management Information: Administrative personnel (including CEO and CFO) may have access to this information, but all other employees may not.

Reputation: All personnel represent our reputation. Therefore, any employee can put the company's reputation at risk.

Potential ways to gain access to inappropriate information are to gain access to another user's ID and password. Inappropriate access could be used to misappropriate funds or to damage an individual or a company. We sincerely hope that, in our small company, we would be well aware of such a risk. As the company grows, we will need to find additional ways to be aware of personnel risks other than by close association.

OUTSIDER THREAT VECTOR FOR CROWN JEWEL

An outside threat to our customer and product information is intrusion via the internet. It is possible that internet access could allow IP address spoofing and port scanning. As network traffic flows between the web server and Network2, access to files could damage our reputation. Additionally, if a malicious individual was able to gain access to our internal network, severe damage to files via copying, modifying or deleting could cause irreparable damage to our reputation. It could also cost us severe penalties and liability costs for lost funds.

Several mechanisms are in place to protect computers located on the DMZ and Internal Network from intrusions. For the DMZ, filtering rules are in place on the router that connects the DMZ to the Internet to prevent IP address spoofing and port scanning. In addition, server hardening measures and IP filtering rules have been implemented to the server from the Internet and to control the types of network traffic allowed between the web server and Network2.[3]

In general, we would suspect that our data is valuable because of access to high dollar funds. However, because our company is very small, it is anticipated that it would be more likely that we would be found by accident via port scanning rather than deliberately attacked.

MALICIOUS CODE THREAT VECTOR FOR CROWN JEWEL

Though the NIMDA worm has dropped off as a recent threat, it is a good example of the types of threats that face our company. According to Symantec:

> W32.Nimda.A@mm is a mass-mailing worm that uses multiple methods to spread itself. The name of the virus came from the reversed spelling of "admin."
>
> This worm:
>
> - Sends itself by email
> - Searches for open network shares
> - Attempts to copy itself to unpatched or already vulnerable Microsoft IIS web servers
> - Is a virus infecting both local files and files on remote network shares. [4]

NIMDA, and similar worms, compromise security settings and replace legitimate files with itself, thus propagating further damage.

Worms can be spread to our network via our dial-up access. Computers in-house are protected by anti-virus software, but protection relies upon virus definitions being up-to-date. If a user has been on the road for a period of time, it is possible that their virus definitions have not been updated. When a user logs in their laptop via direct connection to the network, anti-virus definitions are automatically updated. But, for a dial-up users, they must remember to update

[3] Plank, Richard. "Technical Risk Analysis." Company Confidential Publication. July 13, 2004.

[4] "Symantec Security Response." July 30, 2004. Symantec. URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html (September 20, 2004).

their definitions themselves. Therefore, a dial-up user could infect our internal network.

The results of such an occurrence would be severe damage to our ability to function. The propagation and cleansing of the worm would need to be quick and decisive. We have established an internal incident response policy which gives the technical experts authority to do whatever is necessary to prevent malicious code spread.

GIAC'S MOST SEVERE THREAT

As described above, worms and viruses are a severe threat to GIAC. Interestingly, it is our own employees who are most likely to infect us. This threat is not only somewhat likely to occur, it **has** occurred! Recently. An employee who travels frequently, and for long periods of time, dialed into the network and we received a relatively harmless worm.

The potential damage is great. If files are lost or damaged, or if information is extracted and released to malicious individuals, serious harm could come to our customers and to our reputation.

REMEDIATION STRATEGY

The remediation strategy is two-fold. First, we need to implement a virus definition check upon every dial-up connection. Users should not be allowed access to the network without an up-to-date virus definition. Users should be informed that they cannot access the network due to out-of-date virus definitions. Users can then call the Help Desk for assistance in getting their definitions current.

A second strategy is to have a good backup plan. If files are damaged, they could then be retrieved from the backup. It is less than ideal to retrieve backup files because some work and data will inevitably have been lost. It is preferable to avoid damage before it occurs.

A backup plan is already in place, as described below. However, it will take a system administrator to implement the virus definition checking. Our current anti-virus software has the ability to check definitions as part of the login procedure. It will take about one week of dedicated time for the system administrator to make changes to the startup procedure and test the changes. At this point, we do not estimate any purchases to be made. Total cost is labor only. At a rate of $75 hour (chargeable rate includes benefits), the total cost to implement is $3000. The risk reduction is well worth this low cost of implementation.

BACKUP STRATEGY

Most of the company's critical information is stored on the network because of the high need to share information. However, some data is stored on local drives because of the convenience associated with storing information locally, particularly on laptop computers.

GIAC's standard practice for backup is to establish a daily, weekly and quarterly backup schedule for all of the network-based servers. Typically, daily backup sets are created Monday through Thursday and recycled each week. Weekly backup sets are created every Friday and are recycled every three weeks. Quarterly backups are generated on the last weekend of the calendar quarter and are recycled after eight quarters.[5]

GIAC Enterprises uses the ArcServe backup utility to perform its backup operations for our servers. This utility can be configured to perform regular backups of hard drive information. It is recommended that GIAC backs up hard drives on a weekly basis automatically using this utility. Since our company is very small and there are few computers to backup, we do not anticipate needing to increase our tape or tape drive capacity. Implementation of this strategy should be relatively inexpensive.

In addition, uses should be educated about back up policies and procedures, paying particular attention to the benefits of storing information on the network. Although it is difficult to change company practice, some education may still prove to be helpful in beginning to work toward a positive change. A weekly backup protects GIAC from a catastrophic loss of data, while it still may be painful for the user to repeat a week's worth of work. Therefore, after an employee or two experiences a hard drive failure, it may be more likely than others will store critical information on the network where it is backed up daily.

To restore a hard drive after a failure, the following steps should be taken to make the server operational and to recover the most current data:

- replace the affected hardware
- reinstall the operating system
- restore the files from the most recent weekly backup tape
- restore the files from the most recent daily tape
- manually re-enter any orphan transactions (data that was entered after the last backup operation)[6]

[5] Neufeld, Tim, Richard Plank, John Swartzendruber. "Daily Backup Practices." Company Confidential Publication. Created June 5, 2001, Revised July 12, 2004.

[6] Ibid.

OFFSITE BACKUPS

Duplicates of our backups need to be created. At a high level, GIAC needs to find a location to store tapes off-site. A business located across the street from GIAC has an equipment shelter which is FEMA rated for tornado and snow storms. They built this facility in the last four years to use as an alternate work site in case of disaster. It would be a simple matter to ask if we could store our tapes in their facility.

One time tasks to start this process would be to:

1. Estimate the amount of time to create duplicate backups. Should we consider a dual tape drive to reduce backup time?

2. Inquire of our business neighbor if we may use their facility for tape storage.

3. Develop a schedule for transporting tapes.

4. Develop a safe method for transporting tapes.

A locked safe placed in the equipment shelter would likely be adequate to protect the tapes. The equipment shelter is always locked, even during normal business hours, and only limited personnel are authorized to enter. We would want to have some agreement with our business neighbor about the protection of our assets.

We would also need to request access to the equipment shelter so that our staff could access our tapes in the event that we must perform a recovery.

APPROACH TO BUSINESS CONTINUITY PLANNING

In general, developing a business continuity plan (BCP) is a large undertaking. There are several key items that must be included in a BCP:

1. Identifying a crisis management team

2. Identifying impacted areas

3. Identifying critical services that must be available in order for the company to function. A business impact analysis is helpful in determining priority of service restoration.

4. Having adequate backup and storage of backups (as identified in the above two sections).

5. Identifying risks to the business, both technical and non-technical. Some of these aspects have been covered in the section above entitled “Insider Threat Vectors…”

6. All systems should be well documented and procedures should be in place for restoration of systems, particularly critical systems.

7. Key personnel and contact information should be documented.

8. All essential documentation for restoration and contact information should be printed and kept in multiple locations. For our small company, I would recommend that key personnel take copies to their homes with them and keep them in a personal safe (could be provided by the company).

After development of a high level plan, a scenario test should be conducted. The team should spend a day talking through several possible scenarios and identifying what actions need to take place to restore operations. While this approach is not completely thorough, for our organization it is the most cost effective.

As GIAC Enterprises grow, the BCP should be reviewed annually to cover new business areas. New business impact analyses will need to be performed. Changes to the recovery priority and plan will need to be updated. Documenting is an on-going task, and to cover all IT operations we will need to do some documentation on a regular basis.

If GIAC Enterprises BCP is inadequate, then attention should be given to it promptly. It is not necessarily a popular project. However, if the company should be a position to put their BCP in action, we will be glad we put appropriate effort into creating a usable and accessible plan.

REFERENCES

“Building a Comprehensive Disaster Recovery Plan.” Info-Tech Research Group, September 2003. (15-33).

“CISCO Threat Defense System Guide: How to Provide Effective Worm Mitigation.” April 2004. CISCO Systems. URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns441/c654/cdccont_0900aecd800f714e.pdf (September 20, 2004).

Neufeld, Tim, Richard Plank, John Swartzendruber. “Daily Backup Practices.” Company Confidential Publication. Created June 5, 2001, Revised July 12, 2004.

Plank, Richard. “Technical Risk Analysis.” Company Confidential Publication. July 13, 2004.

Small, Bob. “Engineering Secure Systems Using Threat Modeling.” April 2004. Software Productivity Consortium NFP, Inc. URL: http://www.software.org/pub/externalpapers/sstc2004_small2.pdf (September 20, 2004).

“Symantec Security Response.” July 30, 2004. Symantec. URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html (September 20, 2004).

“Top Ten Malicious Code Threats for September 2003.” June 1, 2004. National Institute of Environmental Health Sciences. URL: http://www.niehs.nih.gov/isso/malicious-0903b.htm (September 20,2004).