Global Information Assurance Certification Paper

Gigantic Inflatable Airworthy Contraptions Enterprises

Security Assessment for GIAC Enterprises

Written by Carla Brinker

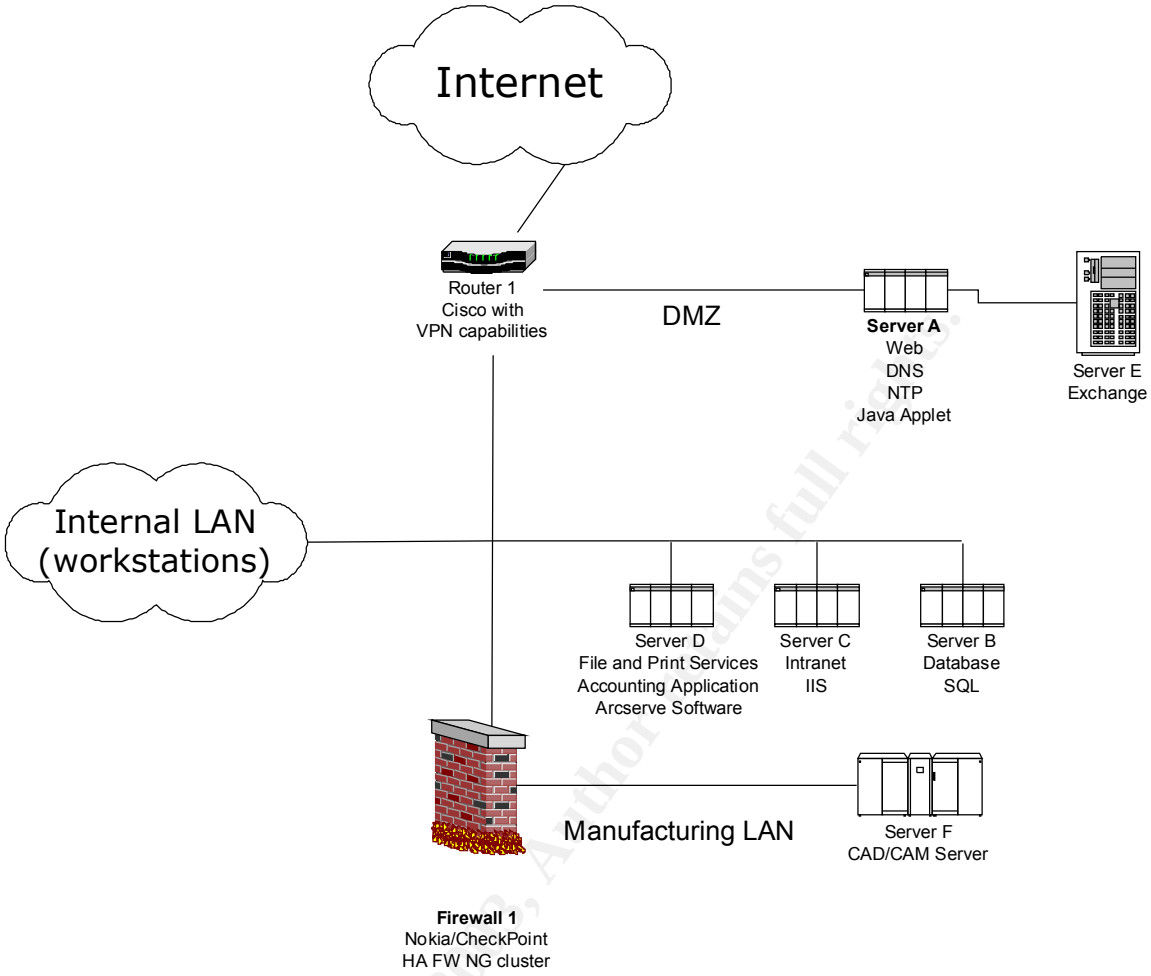
Abstract
GIAC Enterprises (Gigantic Inflatable Airworthy Contraptions Enterprises) is a fictitious state-of-the-art hot air balloon manufacturer. This paper will present the business environment and technology of GIAC. This paper will also identify three areas of risk that exist on the network: inadequate backup procedures, improper management of the router, and an unpatched IIS server residing in the DMZ. Further, I will evaluate a Backup Policy and present a revision of the policy that will comply with GIAC's needs. The last section of the paper will contain a procedure that supports the revised Backup policy and works to mitigate one of the risks on the network.

Assignment 1
Business Description
GIAC Enterprises is a leading high tech designer and manufacturer of hot air balloons in the world. The GIAC corporate office is in Houston, Texas. The corporate office building is divided into office space area and a manufacturing plant. Due to the high tech environment, GIAC Enterprises only requires 33 employees. Directors of Sales and Marketing, Information Technology, Accounting, Design and Manufacturing departments report to the CEO and the President of the company directly. The Information Technology department supports all other departments, including the CAD/CAM (Computer Assisted Design/ Manufacturing) system in the manufacturing plant.

GIAC's customer-base is very small. Since a hot air balloon requires a pilot's license to be flown, this limits the number of people that could be potential GIAC customers.

Employees do not have remote access to the local network, but certain B2B (Business to Business) operations are conducted over VPN (Virtual Private Networks) connections. For example, GIAC Enterprises uses an EDI (Electronic Data Interchange) system to work with suppliers and transportation companies.

IT Infrastructure
The network diagram is included below.



The network consists of 6 servers: Server A, Server B, Server C, Server D, Server E, and Server F. The servers are housed in a secure server room within the company. The server room is protected with badge card readers to allow greater physical security for the servers. Only 3 people have access: The CIO (Chief Information Officer), the Systems Administrator, and the Backup Systems Administrator. The server room is cooled by two redundant air-conditioning systems, each independently capable of cooling the entire room during a hot Houston summer.

Servers on the Internal LAN

Server B is used for storing the company database. It is a Dell PowerEdge server, running Windows 2000 server, fully patched, with only the necessary components installed. The database software is Microsoft SQL server and is also fully patched. The server's configuration follows the principle of least privilege[1]

[1] http://hissa.nist.gov/rbac/paper/node5.html

(users are only allowed access to those files which they require to perform their job). Server C is a Dell PowerEdge server and serves as the internal web server (or intranet server) also running Windows 2000 server and IIS 5.0. Only the necessary components are installed and the principle of least privilege is enforced. Windows 2000 and IIS 5.0 have been patched with the latest patches. The server houses the intranet site, which contains employee phone lists, balloon templates, balloon specifications, pricing formulas, and vendor information. The intranet server is not allowed to communicate with the web server in the DMZ. Server D is the file and print server and also houses the home directories of the users. Server D serves as the root of the Active Directory tree. The server is a Dell PowerEdge server and runs Windows 2000 and is actively patched. Only the minimum required Windows components have been installed (IIS is not installed on this server because it is not required). An accounting application (Numbers Calc) is installed on this server and each month a status check is performed to verify if any upgrades or patches are available. A search of vulnerability databases[2] did not reveal any known vulnerabilities. The accounting application (Numbers Calc) includes its own authentication and access controls and is maintained by the Accounting Department. Server D also houses the backup software (Arcserve) and the tape drive.

The workstations for the users are also located on the Internal LAN. The workstations are all standard installations of Windows 2000 Professional. The workstations do not include modems and are installed with only the minimum required services. Users are not allowed to store data on their local drives. This is mandated by the Windows Group Policy and cannot be overridden without Administrator permissions.

Server F is the CAD/CAM server. It is running the SUN operating system and is maintained by an outside consulting firm. The consulting firm is under a strict NDA (non disclosure agreement). The firm also applies patches on a monthly basis and secures newly discovered vulnerabilities. If a vulnerability is revealed that is not internet-based and poses a threat due to of from internal users, the firm is required to correct that vulnerability within 3 days. If the vulnerability is internet-based, the firm is required to correct it within 30 days. Since this is an internal server that does not access the Internet and is provided protection from the firewall and router, a longer period of delay for applying any patches is considered an acceptable risk for this organization based on its history.

Servers in the DMZ

Server A is a Dell PowerEdge server and serves as the internet-facing web server. It is a Windows 2000 server with only the necessary components installed (this does NOT include an FTP server due to the insecure nature of FTP). It is running IIS 5.0 in its default configuration and has not been patched since the release of Windows 2000 Service Pack 1, due to the staff being busy with other

[2] http://www.cert.org/nav/index_red.html and www.securityfocus.com/bid

obligations. Server A is the main entry point for all Internet users who are looking for information pertaining to the sport of hot air ballooning. Pilots are able to place orders via a customized Java applet called Fly In. A search of popular vulnerability databases[3] did not reveal any known vulnerabilities for this application. The router is configured to allow communications between Server A and Server B (the server that houses the SQL database). This allows the input collected from the web page to be stored behind another layer of protection (the router). The DNS Services are provided with the Windows 2000 server software. It serves both the internal and external DNS requests on the network. This server also houses NTP (Network Time Protocol). NTP is installed on the server to help synchronize the time throughout the network to allow for more thorough log analysis. A Snort NIDS (Network-based Intrusion Detection System) is planned for the near future. NTP is installed in anticipation of the NIDS.

Server E is also a Dell PowerEdge server and serves as the mail server. It is a Windows 2000 server, running Windows Exchange server. It does not participate in a domain or tree with other servers and is a stand-alone server. The server is configured in a hardened state following the SANS Step-by-step guide for Windows 2000.[4] The Exchange server has also been configured using the hardening tool called Symantec DeepSight Analyzer.[5] Both the operating system and the email server are patched in a timely manner. This server also houses McAfee anti-virus software version 7.0[6], which scans incoming and outgoing messages for viruses.

The router (Router 1) that creates the DMZ is a Cisco 3660 and is also used to establish a VPN that allows EDI (Electronic Data Interchange) to travel between suppliers and the company. The router is configured to allow in Internet traffic on port 80. It also restricts traffic to the internal LAN by denying all externally originated traffic and allowing in designated IP addresses that reside in the DMZ. The only supplier that uses the VPN is a fabric company that offers the FAA approved fabric and thread required for building hot air balloons. UPS (United Parcel Service) is used to allow for JIT (just in time) delivery and warehousing and therefore does not require a VPN connection. User access to the Internet is limited based on principle of least privilege (only those users that absolutely need the Internet for research are allowed access).

The firewall that creates the Manufacturing LAN (Firewall 1) is a Nokia/CheckPoint HA FW NG cluster (High Availability Firewall Next Generation cluster). The firewall limits incoming traffic to the Manufacturing Segment as well as prevents any traffic from exiting the Manufacturing Segment. This firewall is necessary because the CAD/CAM server is maintained by an outside consulting

[3] http://www.cert.org/nav/index_red.html and www.securityfocus.com/bid
[4] http://store.sans.org/store_item.php?item=22
[5] http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=159
[6] http://www.mcafee.com/myapps/vs7pro/default.asp → McAfee VirusScan Professional 7.0

firm and it is desired that the consulting firm be separated from the rest of the network servers.

A balloon pilot that recently left the company to run his own balloon business previously maintained the firewall and router. A newly hired network administrator has just been hired and is currently attending router administration classes. Her goal is to secure the router upon returning from the offsite classes. At present, no one is maintaining the router or firewall or reviewing the logs.

An additional firewall is planned that will protect from insider attacks. This firewall will increase the defense in depth approach by separating the intranet servers from the users on the internal LAN. This firewall would ideally be configured differently from the existing firewall so that an intruder could not use the same attack to penetrate both firewalls.

The crown jewel of GIAC Enterprises is the SQL database that contains all the balloon designs, design specifications, and customer sales information.

Business Operations

When an order is received via the web site, a salesperson calls to work out the intricate details of the order. Since each hot air balloon is an FAA (Federal Aviation Administration) certified aircraft, many laws apply. The laws are rather detailed and thus, an order cannot be completed via the website. The salesperson is well versed in these laws and keeps them mindful during the order confirmation phone call.

After the salesperson seals the order, payment plans are negotiated. Credit cards are not accepted via the website because the final price cannot be determined until the intricacies of the aircraft are determined and appropriate pricing is applied. Therefore, the credit card or other payment options are established during the final sales call and do not involve network connectivity. (This may seem a daunting task, however, the average year only contains the sale of 20 hot air balloons.) After the salesperson is finished with the phone call, they then create a rough paper mache model of how the balloon should be designed. This is then taken to the CAD/CAM Department. The CAD/CAM operators review the salesperson's work and enter the drawing into the CAD/CAM system. The CAD/CAM system also has a limited system of checks and balances to ensure safety concerns are met. After the extensive process of designing the balloon is complete, the pattern is then printed and stored on a floppy, which is delivered via sneaker net to the Stitching Department and no longer requires the use of the internal network. The Stitching Department uses this diagram to program the robotic sewing machine. The thread is loaded into each spindle based on the colors required for the balloon. The pre-cut pattern pieces are then added to the sewing machine assembly line. The pre-cut pattern pieces are fed into the machine so the machine can maneuver them as needed.

The sewing machine is then programmed internally (it is not networked) to complete the stitching of the balloon. 8 different series of pattern pieces will need to be loaded into the sewing machine throughout the process of stitching the balloon. As each section is added, the balloon begins to take shape. As the balloon is being assembled, 2 Quality Assurance Technicians are supervising the assembly process. (It may seem a bit of overkill to have two people watching a sewing machine, until you consider that a hot air balloon is rather large - 7 stories tall on average). After the balloon is fully assembled, it is quality assurance tested by a certified inspector. After the QA process, it is then attached to a basket and test-inflated. If the balloon is able to withstand the usual inflation process, the balloon is declared complete and a test pilot is scheduled to perform the initial flight of the aircraft before the sale is completed.

The critical software point within this network is the SQL database that is used by the Sales Department. This database contains all customer information, all prospective customer information, the specifications (or laws) for each balloon that are set by the FAA, and the conversion information to load those balloon patterns into the CAD/CAM system. The CAD/CAM system ranks a close second to the Sales database in criticality. The CAD/CAM system is critical to the sewing process, while the Sales database is critical to securing the sale. The sewing machine has its own floppy drive and it reads the CAD/CAM files directly. It does not require any server communication.

Assignment 2

Using the formula for calculating risk (Risk = threat X vulnerability), the top 3 risks to GIAC Enterprises are:

1. Loss of availability caused by inadequate backup procedures
2. Loss of data integrity caused by improper management of the router
3. IIS 5.0 server that is unpatched and residing in the DMZ

Risk 1 - loss of database availability caused by a failed hard drive which was not backed up properly

As mentioned above, the Sales SQL database is a critical part of the network and is considered the crown jewel because of its high level of criticality. This database needs to be backed up in multiple ways to ensure its availability. Currently only one tape drive exists on the network (attached to Server D). It is only capable of backing up one server per night, due to the necessity to change the tape media to accommodate additional servers. SQL Server includes its own backup routines. The SQL server internal backups are scheduled by the database administrator on an hourly basis. However, the resultant backup files are stored on the same physical server as the original database. The server does not utilize a RAID array. If the hard drive containing the database and backups were to fail, there would be days of the week that would not have a recent backup available (due to the tape rotation and limited capacity of the existing tape drive). A timely solution needs to be reached to provide more current

backups so that sales information would not be lost. With the current inadequate backup situation, if a hard drive failed in the server housing the database, the company would not be able to finish the orders they have received and would not be able to effectively market the correct audience to secure new orders. Within a few years, the company's marketing efforts would suffer a decrease in efficacy and the company's reputation would be severely tarnished. The company would most likely dwindle down to nothing and close it doors.

Because of the criticality of the data on the network, mitigation steps should include a tape backup solution with offsite storage that could perform nightly full backups of all servers. The IT Department will implement an external tape drive on the SQL Database Server (Server B). It will have enough capacity to backup the servers in the DMZ and the Internal LAN. The backup software (Arcserve) will include an open file agent that will allow the current SQL Database files to be backed up while in use. The SQL program will continue to generate hourly backups of the database. The backup software should also backup the backup files created by the SQL program. The backups should be scheduled to run nightly and backup each system in full. The backups should be verified each morning in accordance with the company's backup policy. Once verified, the tapes should be sent to a secured offsite storage facility to provide protection from other threats over and above a failed hard drive (such as tornados, floods, fires, etc).

Other means to mitigate this threat would be to include hardware redundancy. A RAID configuration would allow for one drive to fail, while one or more drives continued operating while the failed drive was replaced. The backup solution would be required for any disaster and is therefore the focus of this section.

Although this is not the only threat/risk that pertains to the SQL database, it produces the highest risk at present because many of the other threats/vulnerabilities have already been mitigated.

Risk 2 - loss of data integrity caused by improper management of the router

This risk (loss of integrity) also focuses on the crown jewels – the database, however the threat and vulnerability vectors are different. The router is currently administered by an inexperienced admin. The router was configured years back by an outsourced firm. Little maintenance has been done on this router due to the lack of trained personnel. Because of the lack of attention, the router allows more traffic than it should. The router currently allows ports assigned to common malware, such as BackOrifice (port 31337) and SubSeven (ports 1243, 2772, 2773, 6711, 6776, 7215, 27374, 54283). Even the novice user can execute this small sampling of malicious applications. Since these tools are easily obtainable and require little knowledge for their use, this would create a high threat level and result in this risk occupying the top 3 risks on the network. If such a tool (malware) could penetrate the network because the router is too tolerant,

company confidential information could be changed or destroyed. This would make the ability to communicate with pilots, customers, and vendors extremely difficult, if not impossible (which would ultimately put GIAC out of business if they could not communicate effectively with their clients).

To mitigate this risk, the router will be configured in a more restrictive manner. The router admin is currently away receiving training. When she returns, an outside firm will be hired to determine which ports are necessary. Their goal will be to convert the router from the "allow all unless denied" stance, to "deny all unless specifically approved" stance. This will allow for a firmer network border and will reduce the number of attacks that can penetrate through to the SQL database. The outside firm will work closely with the newly trained admin to help her understand the systems she is caring for and will ensure her ability to properly maintain the router in the near future. The firm will train her to watch for new vulnerabilities and how to combat them with router changes. The firm will also familiarize her with how to read the logs and how to rule out what is typical traffic versus traffic of interest. With a more well trained router admin, the router will retain is heightened level of security that the outside firm will achieve.

Loss of integrity = Malware X improper configuration of the router

Risk 3 – loss of data integrity and confidentiality due to an IIS 5.0 server that is unpatched and residing in the DMZ

The IIS 5.0 server that resides in the DMZ is a large concern to the corporation because of the visibility it has. This server is responsible for their image on the Internet. This server is readily accessible from the Internet. As stated above, it also interfaces with the SQL database on the intranet. Since this server is Internet-facing, the threat comes from unknown outsiders with malicious intent to gain the information contained within the SQL server. IIS is known for its many vulnerabilities that often remain unaddressed by Microsoft for lengthy periods of time. Because of IIS's reputation, this threat/vulnerability pair creates one of the top 3 risks on the network.

This server is not properly maintained and has not received the latest patches that were released to address recently identified vulnerabilities. The vulnerability most applicable to this server would be trendy worms that seek out unpatched servers to exploit. If this server falls to an attacker and is controlled, it can be used to target the crown jewels, the Sales SQL Database via the connection that is allowed through the router between these two servers. If an outsider controls the SQL database, it could be modified, copied, or even deleted. If the database was modified, it could be a lifesaving matter. If a balloon specification is set to something outside of the FAA requirements, safety issues could be of concern and in extreme cases lives could be lost. If the database is copied and given to another competing balloon manufacturer, the customer information would be very valuable to that other company. If the database was deleted, it would be impossible for the company to function, since this is the central repository of the

company information. If an outsider with malicious intent accesses the database and either modified, deleted, or copied, the company's future would be in jeopardy. The ballooning industry is very fragile. There is not a lot of demand and any negative events will harm the company's reputation and most likely, put it out of business in a few years.

In order to mitigate this threat, the IIS server will be maintained by a member of the IT Staff. The IT Staff has drawn up a policy (Server Maintenance Policy) that states the IIS server will be patched within 2 weeks of a release of a patch that pertains to the software installed on this server (both operating system and web server patches). The IT Staff will collect information they receive from SARA (Security Auditor's Research Assistant)[7]. SARA is a service that allows you to request only those security bulletins that pertain to the software installed on your network. This helps filter out those bulletins that do not pertain to you. The IT Staff will comply with the policy by installing the patch on an offline, un-networked test system. After performing beta testing on the test system, the patch is deemed "authorized for production status" and applied to the production server.

By staying up-to-date on patches, the very high threat of outsider attack becomes very low because the number of known existing vulnerabilities will be dramatically decreased.

Assignment 3

The policy under review is taken from http://www.ca.sandia.gov/cacplant/backup.php. The evaluated policy appears in Appendix A (only the company name and minor typos have been changed). This policy is meant to assist in mitigating the problem in Risk 1 of Assignment 2.

Overall, the policy is lacking organization and content. Since the policy lacks subtitles, I have included the statements from the policy that I felt pertained to each section. The original policy content is indicated in italics.

Purpose
The following data backup configuration for GIAC Enterprises has been set to satisfy the GIAC Production Computing Requirements.

This content is as close to a purpose statement that can be found in the policy. This section is lacking a clear, distinct function for this policy because the phrase “Production Computing Requirements” is not defined. Although the policy is to support the GIAC Production Computing Requirements, this information is more appropriate for the Background Section of the policy. This sentence should be

[7] www.www-arc.com/sara

replaced with a statement that addresses why the policy is needed and what it is going to accomplish.

Background
The following data backup configuration for GIAC Enterprises has been set to satisfy the GIAC Production Computing Requirements.

Although this material was explained in the Purpose section, I feel additional comments are necessary to explain how it relates to the Background section. The Background section is to elaborate on the necessity of the policy. Additional information should be included that assists readers in understanding the need for this policy. Additional information might include how essential the data is and how backups are critical to restoring the business operations.

Scope

GIAC Enterprises Production Systems is comprised of cluster systems in three networks: SON, SRN, and SCN. Each network environment offers a central data repository for user files served by a Network Appliance Filer which provides a network file system service (NFS), containing hundreds of gigabytes of data storage to each and every node within the Cplant cluster. The Network Appliance disk storage is comprised of a fiber channel RAID level 4 system to ensure data integrity.

Each of the three Network Appliance Filers are configured to create snapshots on an hourly, daily, and weekly basis. A snapshot is an online read-only copy of the entire file system.

This Scope section pertains more to machines rather than people. Although the machine aspect is important, the people are the ones going to enforce or abide by the policy. It is a good idea to include those machines that are covered by the policy as well. However, by indicating specific machines by name, this policy can become out-of-date quickly as machine names change or machines are added. A more comprehensive scope is required that covers all machines. By using a more focused scope, explaining the terms used (SON, SRN, and SCN) will not be necessary. The scope should identify which roles and/or departments are expected to adhere to this policy.

Policy Statement
The schedule of snapshots is as follows:

- *Weekly done every Sunday at midnight and the system keeps the 2 most recent.*
- *Daily done every night at midnight (except Sunday) and the system keeps the most recent.*
- *Hourly done at 8am, Noon, 4pm, and 8pm and keeps the 8 most recent.*

Tape backups are done weekly and monthly to supplement the online snapshot data backups and assure data restoration capability if a major disk failure occurs. These tape backups are done either automatically or interactively. A monthly tape backup is a complete dump of the entire file system and done on the last weekend of every month; a weekly tape backup is an incremental dump of all file changes that have occurred since the previous monthly tape backup and occur every Friday evening. Monthly tapes are held for one year and weekly tapes are held for 8 weeks. Tapes are stored in a locked cabinet.

Recovery of old versions of files due to accidental changes or deletions can be made by any user from a Filer snapshot. The snapshot feature enables users to restore their own files without help, because files in snapshots can be viewed and copied by those who have permission to do so with the original files. Tape backup file restoration would be required if the changed or deleted file is older than two weeks and would require a request to a GIAC Enterprises system administrator for recovery.

Although the GIAC Enterprises network does not utilize Network Appliance or the Filer features, this policy still has some policy statements that can be applied to GIAC, however many of the policy statements are better suited in a procedure than in a policy. For instance, the schedule of snapshots would be a good starting point for writing a procedure that pertains to the tape backup structure that GIAC needs to implement. The policy should be modified to include clear statements of how the backups must be performed, to include such guidelines as the frequency of the backups. The SQL backups that are performed should be covered in a separate policy that pertains to just the SQL Administrator. Such a policy would include additional responsibilities such as auditing user permissions, using a different account than SA, etc. Such a policy would cover the backups, but also a great deal of other issues that are unrelated to the Tape Backup Policy.

The section that includes the definitions for each type of backup would be helpful in a policy if anything but a full backup was being used. In this case, the revised policy calls for full backups to be performed nightly to allow for rapid restoration if a major disk failure occurs and a definition is not required.

The information pertaining to tape retention is also useful. This portion of the policy can be used to establish the requirement for secure offsite storage.

The policy mentions users requesting files to be restored. Again, this is something that should be covered in separate, supporting policy that addresses all users rather than just the IT Department. Since the scope is different, a separate policy is required. The details pertaining to restores should be defined in a supporting procedure. The procedure should define timelines for restore requests, responsibility for restores, etc. This information is not appropriate for a

backup policy. Policy is to cover who, what, and why. A procedure is to cover when, how, and where. These details would fall more into the how category.

Additional policy statements are required to bring this policy into accordance with GIAC's needs. For instance, test restores should be required monthly to ensure the tape backup process is working. A backup is only as good as your last restore. Without verification that these backups are truly working and not just creating log entries, restores must be performed on a periodic basis.

Responsibility
There is no mention of responsibility in this policy. The policy does not mention who endorses or maintains the policy, nor who will carry out the policy and ensure its compliance is met. These are both items that should be added to the revised policy. The CEO is responsible for approving and endorsing this policy. The IT Director is responsible for updating this policy on a yearly basis.

Action
This policy does not have any content that would be suited for an Action section. The Action section should include what will happen if this policy is not followed. Since a policy is meant to be a firm set of standards and compliance is mandatory, the Action section should state what non-compliance would bring to the user. This would include anything from a short probation up to and including termination (depending on the severity of the violation).

Revised Security Policy

Server Data Backup and Retention Policy Version 1.3

Approved by: Chief Executive Officer on March 17, 2003
Effective date: March 24, 2003
The policy will be re-evaluated March 17, 2004 by the IT Director

Purpose
This policy is the governing rules pertaining to the server's data backup and retention of GIAC Enterprises. This policy will cover all data stored on network servers and will define how data will be backed up and stored to allow for the best possibility of being able to recover the backed up data.

Background
This policy has been established to reduce the losses we have recently experienced due to files being deleted and overwritten in error and also to fulfill the GIAC Production Computing Requirements. By ensuring our data is backed up in a timely manner, we will be able to restore data rapidly if an unforeseen event occurs.

Scope
This policy applies to all IT Department Staff and all networked servers. As stated in the Acceptable Use Policy (www.giac.com/intranet/policies/acceptableuse.pdf), all user files are to be stored on the network and therefore this policy will not pertain to individual workstations. The IT Department will apply these guidelines to ensure adequate backups of networked servers are secured.

Policy Statement

- All servers will be backed up each weekday night
- All backups will begin at 6pm
- The backups are to be full backups of every file on the networked servers to allow for rapid restoration in the event of a major disk failure
- Open file agents are to be used to allow for the backup of open files
- Each business day morning, the backups will be verified by reviewing the logs for error messages. All error messages are to be resolved. If resolution is not possible resulting in a file or server not being backed up, the IT Director must be notified before 3pm.
- Once the backups are verified, each tape will be labeled with the server(s) that are on that tape, the software that was used to create the backup, the version of that software, and today's date in dd/mm/yyyy format. The tape bar code number is to be recorded in the Backup Inventory Log along with today's date.
- Once the tapes are properly labeled and inventoried, they are to be sent offsite via The Shuttle Company. The Shuttle Company is under a strict contract and will ensure the safety of our critical data. (www.giac.com/intranet/policies/ShuttleCompany.pdf)
- The Shuttle Company will drop off the scheduled tapes that will be used for the next day's backup.
- Month end tapes will be held for one year and weekend tapes will be held for 8 weeks.
- A test restore will be performed monthly to ensure the backup process is working (in accordance with the Disaster Recovery Policy).
- A yearly audit will be performed to verify and cleanup the tapes that are stored at the offsite facility.
- Tape drives will be cleaned on a weekly basis.

Responsibility
The Backup Administrator is responsible for verifying each automated backup job has completed. The Backup Administrator is also in charge of swapping tapes, handling The Shuttle Company's existing contract, and handling any request for restoration of data from those tapes. The Backup Administrator is responsible for alerting management if the existing hardware/software is no longer adequate and additional resources are required.

The CEO is responsible for approving and endorsing this policy. The IT Director is responsible for updating this policy on a yearly basis. The IT Director will also perform unannounced audits of this procedure to ensure its efficacy.

Action
This backup policy applies to all network servers without exception. Any IT Staff Member that is filling the role of Backup Administrator and fails to comply with this policy will be reprimanded. Reprimands may include anything from probation up to and including termination (depending on the severity of the violation). The IT Director and CEO will determine the level of reprimand in accordance with the Human Resources policies (www.giac.com/intranet/policies/private/HR/Reprimands.pdf).

Revision History
Version 1.0 – initial approval March 15, 2000
Version 1.1 – approved March 17, 2001
Version 1.1a – revised November 14, 2001
Version 1.2 – approved February 1, 2002
Version 1.3 – approved March 17, 2003

Assignment 4

This procedure is used to support the Server Data Backup and Retention Policy version 1.3. It is to be performed daily by the Backup Administrator. In the event the Backup Administrator is absent, the IT Director will appointment an Acting Backup Administrator.

Backup Verification Procedure

* At the start of each business day, login as Administrator to the IT workstation that has Arcserve installed.
* Begin the Arcserve Management Console.
* The job queue will open automatically. Here you will see a job for each server.
* Verify the Next Run field for each job is today's date. If it is not today's date, this is an indication the job did not complete successfully and further investigation is required.
* Highlight the first job. Click on the log icon in the task bar. The log will appear. Scroll carefully through this log verifying that no errors are reported. Open files should have a "successfully backed up" message after them. This will indicate that the open file agent is indeed working and a snapshot of the file has been saved to tape. After reviewing the log, if no errors are found, repeat this process for each job in the queue. If errors are found, attempt to rerun the backup immediately. Click the green stoplight icon to submit the job to run immediately. If the job begins, review the logs when complete. If the job fails to complete, consult the Arcserve Owner's Manual in the Data Center. All errors are to be resolved. If they cannot be resolved by 3pm that day, the IT Director will provide additional guidance on steps that should be taken for that day. The IT Director

will consider the entire scenario before making recommendations on how to proceed. These decisions will be based on the criticality of the file or server missed.
* For all successfully completed jobs, record the completion time in the Backup Inventory log, which can be found at www.giac.com/intranet/policies/backups/Backup Inventory Log.pdf
* Record how much data was backed up. This can help detect if the logs are accurate. This data will be used to benchmark a server and give early indications if the tape drive is nearing its capacity.
* Place a checkmark next to the server if the backups have completed without incident. If there are any concerns (sharp increase in the amount of data backed up, files that could not be backed up, lack of permissions, hardware failure, etc), note this on the checklist.
* Record the bar code number of the tape on the checklist.
* After completely this procedure for each server, submit the checklist to the IT Director before 3pm each day.
* Once the checklist is submitted, swap out the tape in the tape drive using the tape that was delivered via the courier on the previous business day.
* Place the backup tape that has just completed in the secured storage device and take it to the Reception Desk. This device will be picked up by the courier service. (Details relating to the courier service can be found in the "Backup Courier Service Agreement" (www.giac.com/intranet/policies/ShuttleCompany.pdf). The courier is under contract to protect our data while it is in transit between our facility and the storage facility.)

Miscellaneous Notes (not part of the procedure)
Other procedures do exist that support this policy (such as a restore procedure, a restore request procedure for end users, auditing the inventory of tapes at the offsite storage facility, retaining weekly and monthly tapes for archival retention purposes, tape drive cleaning, periodic unannounced audits, etc).

References

Principle of Least Privilege – authored by John Barkley, January 9, 1995 - http://hissa.nist.gov/rbac/paper/node5.html

Security Focus - Microsoft Vulnerabilities – updated daily - http://www.securityfocus.com/bid

Carnegie Mellon Software Engineering Institute - Vulnerabilities, Incidents, and Fixes - http://www.cert.org/nav/index_red.html - updated daily

Symantec DeepSight Analyzer – author and publication date unknown http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=159

The SANS Institute BookStore – Securing Windows 2000: Step-by-Step http://store.sans.org/store_item.php?item=22

Cplant Data Backup Policy, http://www.ca.sandia.gov/cacplant/backup.php Author and publication date unknown

McAfee VirusScan Professional 7.0 - http://www.mcafee.com/myapps/vs7pro/default.asp

SARA (Security Auditor's Research Assistant) – www.www-arc.com/sara/ - Advanced Research Corporation – August 15, 2002

APPENDIX A

Data Backup Policy

The following data backup configuration for The Company has been set to satisfy The Company Production Computing Requirements.

The Company Production Systems comprise of cluster systems in three networks: SON, SRN, and SCN. Each network environment offers a central data repository for user files served by a Network Appliance Filer which provides a network file system service (NFS), containing hundreds of gigabytes of data storage to each and every node within The Company cluster. The Network Appliance disk storage comprises of a fiber channel RAID level 4 system to ensure data integrity.

Each of the three Network Appliance Filers are configured to create snapshots on an hourly, daily and weekly basis. A snapshot is an online read-only copy of the entire file system.

The schedule of snapshots is as follows:

* Weekly done every Sunday at midnight and the system keeps the 2 most recent.

* Daily done every night at midnight (except Sunday) and the system keeps the 6 most recent.

* Hourly done at 8am, Noon, 4pm, and 8pm and keeps the 8 most recent.

Tape backups are done weekly and monthly to supplement the online snapshot data backups and assure data restoration capability if a major disk failure occurs. These tape backups are done either automatically or interactively. A monthly tape backup is a complete dump of the entire file system and done on the last weekend of every month; a weekly tape backup is an incremental dump of all file changes that have occurred since the previous monthly tape backup and occur every Friday evening. Monthly tapes are held for one year and weekly tapes are held for 8 weeks. Tapes are stored in a locked cabinet.

Recovery of old versions of files due to accidental changes or deletions can be made by any user from a Filer snapshot. The snapshot feature enables users to restore their own files without help, because files in snapshots can be viewed and copied by those who have permission to do so with the original files. Tape backup file restorations would be required if the changed or deleted file is older than two weeks and would require a request to a Company system administrator for recovery.