Global Information Assurance Certification Paper

GIAC ENTERPRISES – DATA BACKUP SECURITY POLICIES AND PROCEDURES

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

Martin A. Reymer
SANS Tyson's Corner

Submitted May 7, 2002

TABLE OF CONTENTS

DESCRIPTION OF GIAC ENTERPRISES

GIAC Enterprises (GE) is a global manufacturer of mass storage solutions for small, medium and large-scale applications to the computer industry. GE has existing business relationships with vendors and suppliers of electrical components, mechanical components, drive assemblies, shipping companies and various alliances with distribution companies to market their products. GE also has customers that will use their products to incorporate with the customer's hardware and software solutions as well as the support of those systems to the end users of their products.

GIAC ENTERPRISES IT INFRASTRUCTURE

Protecting the GE network from the rest of the world is the first responsibility of GE's Cisco 3600-series router configured with IP filtering capabilities (see Figure 1). The router has been configured with the guidance of third-party professional consultants, an article from SANS reading room written by Scott Winters, August 15, 2000 entitled "Securing the Perimeter with Cisco IOS 12 Routers", and various articles available from Cisco's support website.

The next layer of protection in GE's network is the Watchguard firewall. It employs security proxies and dynamic stateful packet filtering [1]to be able to manage the information flow through the firewall. Its primary purpose is to guard the external network servers that are available to both the outside world and internal network. There are three servers consisting of Compaq Proliant DL580 rack-mounted servers supporting an external web server running MS IIS 5.0, an external mail server running MS Exchange 5.5 SP4 and an external DNS server running Metainfo, Inc.'s MetaIP DNS product.

The third layer of defense in GE's network is a second Watchguard firewall. It is responsible for allowing information flow control between GE's primary network, the corporate external servers and the Internet. Both Watchguard firewalls are managed from a control PC located on the network's primary segment. This control PC is responsible for logging messages from three firewalls, a Cisco 3600 router, and all error reporting from GE's Compaq servers.

GE's primary network segment is responsible for supporting five primary servers; one Compaq Proliant DL760 data backup server configured with dual fibre channel host bus adapters connecting it to a Smart Array Cluster Storage device, one Compaq ProLiant DL760 internal web server running MS IIS 5.0, one Compaq ProLiant DL380 internal mail server running MS Exchange 5.5 SP4, one Compaq ProLiant DL380 internal name server running Metainfo, Inc.'s MetaIP DNS product and one Compaq ProLiant DL760 data base server running MS SQL 7.0. GE's primary segment utilizes Cisco 3548

[1] Watchguard Technologies, Inc.
URL: http://www.watchguard.com/products/wgls.asp (5 May 2002)

switches setup in a redundant fibre channel between each unit. Located on the primary segment are various HP laser printers, Compaq EVO 500 workstations configured with Windows 2000 OS and Windows Office XP desktop software along with several Compaq EVO N600C laptops also configured with Windows 2000 OS and Windows Office XP desktop software.

GE's network supports a separate segment for the Research and Development (R&D) department. Since the computing environment of that department can be volatile at times due to the nature of having to test and benchmark various hardware and software solutions, this network segment is separated from the primary network segment with a third Watchguard firewall. This firewall provides controlled data flow between the R&D segment and the primary segment. The primary server located on the R&D segment is configured identical to the Data Backup server located on the primary segment. This not only provides redundancy in systems but is often utilized for data restore and verification purposes.

Two major projects under investigation in the IT department are VPN access to network information and implementation of an IDS solution for the network. The VPN access has been requested by the Sales and Marketing groups in order to safely access corporate proprietary information while traveling to customer sites and conducting sales trips, conventions and conferences. The IT department has realized the necessity of having an inside solution that would enable them to provide verification of data flow and access of information. To achieve this the department is pursuing an IDS solution for their network. Figure 1 depicts a VPN connection to the network but is not a total solution at this time.

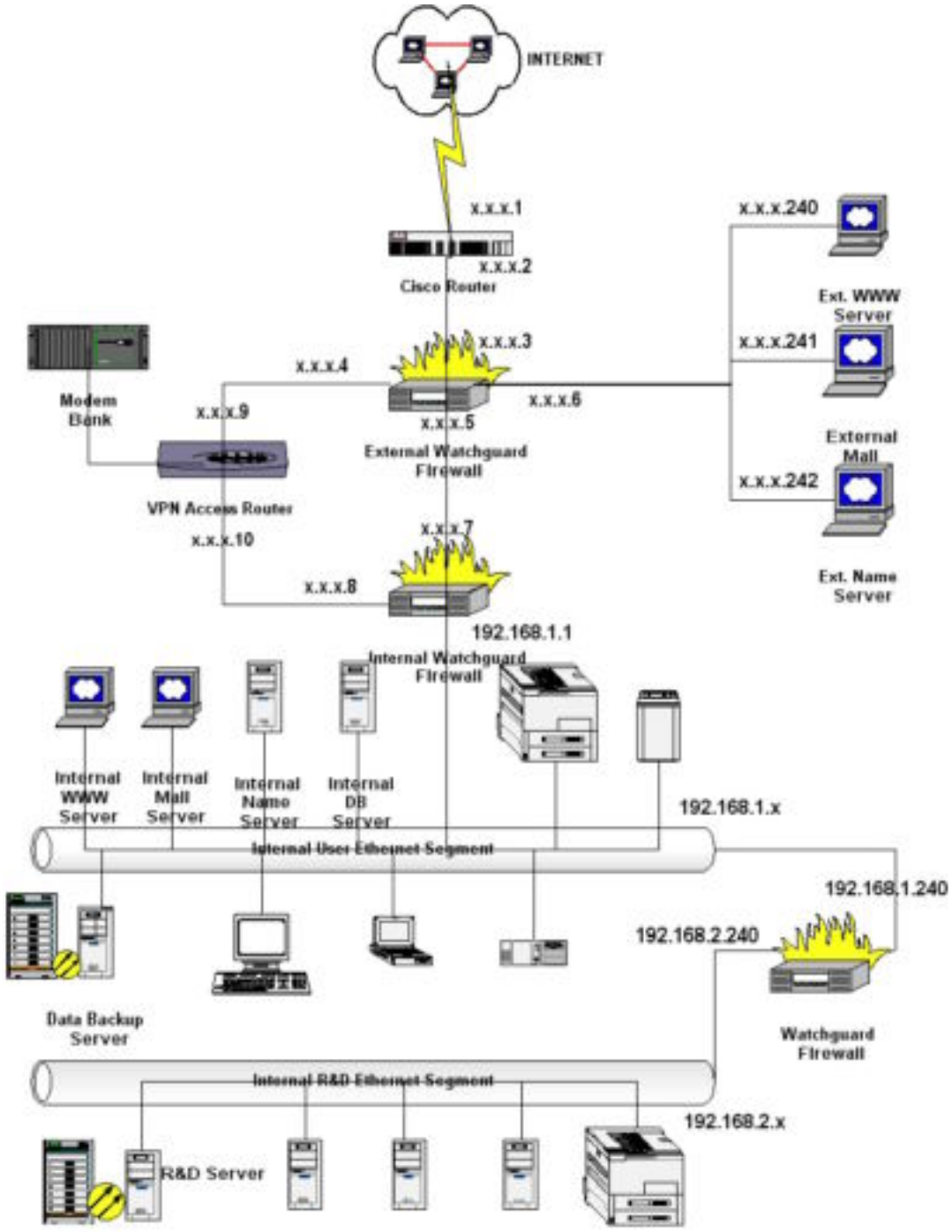

Figure 1. GIAC Enterprises Network Diagram

Business Operations

While the IT group has informed its management of the risk and rewards of running e-Commerce solutions, the IT group is responsible for making information available to GE's customers, suppliers, manufacturers and business partners through its external web server. This information is replicated to the internal web server for redundancy and eventual data backup. Information is also available on the external web server for Sales and Marketing groups related to the products and services that GE provides to the outside world. Depending on the eventual outcome of the VPN solution, the Sales and Marketing groups may have direct access to the corporate proprietary information available on the internal web server and data base server.

The external mail server and external name server provide access for the outside world to contact GE's employees via e-mail. The external mail server relays e-mail to the internal mail server for employee access. It also provides an extra layer of protection for in-bound and out-bound information since both mail servers are not only protected with anti-virus software but filtering content software that block potentially damaging e-mail attachments from entering or leaving GE's network.

Because GE is a manufacturing facility, its employees rely heavily on their internal Enterprise Resource Planning application. The Operations group handles shipping, receiving, warehousing (inventory) and logistics of all materials required to produce GE's many lines of mass storage solutions. The Sales and Marketing group handles all correspondence for domestic and international sales of GE's product lines. The Finance group handles account receivables, accounts payables and all other fiscal responsibilities of keeping a successful company running. The Engineering and Design groups (R&D) have to know what parts are available in order to design, test, benchmark, produce and implement successful mass storage solutions for the various product lines. The Quality group needs access to the manufacturing information, specifications, testing results and production specifications in order to analyze and verify that the equipment is being produced within industry standards.

The IT group is responsible for making sure that the information contained within GE's network; servers, workstations, laptops, network, routers, and firewalls is available to the authorized employees of GE. This includes, but is not limited to;

1. Server configuration and maintenance with Windows 2000 OS SP-2
2. workstation configuration and maintenance with Windows 2000 Professional OS SP-2 and Microsoft Office XP SP-1
3. laptop configuration and maintenance with Windows 2000 Professional OS SP-2 and Microsoft Office XP SP-1 (possibly including the results of VPN solution investigation)
4. printer installation and maintenance
5. firewall configuration, monitoring and software maintenance

6. router configuration, monitoring and software maintenance
7. data backups of all primary servers
8. disaster recovery planning / testing
9. hardware / software requirements
10. help desk support

CRITICAL AREAS OF RISK

Due to the nature of GE's manufacturing processes and capabilities, GE's senior management, as having the highest impact to GE's business, has defined the following areas of concern:

1. Data Backup of All Primary Servers, especially R&D servers
2. Protect Corporate Information from Outside Abuse / Misuse
3. Corruption of the Server Environment

Each of these three areas will be clarified in the following text.

Data Backup / Recovery

Overview of Threat

GIAC Enterprises' servers store information vital to its survival as a prominent player in the global marketplace for providing mass storage solutions to the computer industry. Loss of this information would cause irreparable damage to not only the company in terms of monetary loss, but would be damaging to its reputation and could possibly damage the relationships that GE has with its suppliers, manufacturers and customers as well.

Relevance to GIAC Enterprises

GE's most important assets are their R&D schematics, drawings, specifications and processes, along with their patents and proprietary trade secrets located on its R&D servers. This information is to be protected at all costs. Loss of this information could cause severe downtime resulting in: lost production, delay of product, wasted time in recreation effort, deterioration in customer relationships, loss of market share and inevitably loss in income. In addition to which, GE provides not only internal information to its employees, but information to its external relationships via its external web server. Although this information is protected in part by redundant web servers, the inconvenience and system downtime would still cause unwanted stress and strain in daily business operations.

Potential for Damage

This must be qualified as medium-high to high potential for damage. The IT Group has taken great care to insure that its servers are all protected with appropriate Uniterruptable Power Source (UPS) units. However there are circumstances, natural and man-made, that are out of their control. Any combination of circumstances could cause momentary to catastrophic data interruption or loss.

Likelihood of Exploit

GE's external servers are most likely to incur any of a number of attacks from outside sources due to the nature of having them registered and their network addresses publicly accessible. All GE's servers are based on the Windows 2000 server platform and numerous industry standard publications have stated in the past year that the likelihood of a Windows server being attacked is more than five times that of any other operating system. GE's internal servers are less likely to incur attacks, however, that does not necessarily mean that they can not be attacked from within the primary network. There are numerous types of malicious software that can enter a network through e-mails

and can propagate from PC to PC and even from server to server if not properly protected.

Mitigation

There are several steps that the IT group can take to protect GE's servers and the data contained on those servers:

1. Verify that backup schedules are scheduled after business hours to make sure that users have signed off of their workstations and that all files are closed and available for the nightly backup,
2. Verify that full backups are done on every server located on GE's network and especially R&D's server on a daily basis and separate media are utilized for a period of 31 days,
3. Verify that the full backups are done on a weekly basis and rotated to a separate series of media for a period of 5 weeks,
4. Verify that the full backups are done on a monthly basis and rotated to a separate series of media for a period of 12 months,
5. Verify that the full backups are done on a yearly basis and rotated to a separate series of media for a period of 10 years,
6. Verify that all backups are complete prior to the beginning of the next business day,
7. Verify that records are complete and updated regarding the status of the backups,
8. Verify that all server backup media is stored in the fireproof cabinets and media safes located in the respective server rooms,
9. Having current and up-to-date policies and procedures to follow for data backup, data recovery and server installation.

Overall Vulnerability

GE's senior management realizes that although loss of corporate information contained on its servers could be a catastrophic issue, following the before mentioned processes would bring the issue within an acceptable measure of risk.

Data Protection

Overview of Threat

GE's senior management has come to realize that "if it can happen to the other companies we know and do business with, there is a strong possibility that it can also happen to us!" This reference is applicable to the possibility of having someone or something enter the network and corrupt the information contained on their servers, workstations, routers, and / or firewalls. Basically anything that is capable of retaining data necessary for the survival of GE's systems. Manipulation of data could cause minor annoyances such as Windows rebooting itself whenever you try and accomplish something with the operating system or simply splash some annoying or ridiculous comment on the screen in the middle of a presentation. Someone might even try and manipulate the data on various financial statements and cause the financial department to go absolutely crazy for a couple of weeks trying to find the errors. Risk exists through the manipulation or destruction of data, malicious, willful thoughts of causing chaos within a company, or just waiting to see what kind of information can be obtained from casually looking through the data files on the servers. Unknowingly, the worst damage can be done from within the network by one of GE's own disgruntled employees.

Relevance to GIAC Enterprises

Any data alteration could seriously undermine the efforts of GE's senior management and employees to perform business in the global marketplace. Imagine for a second, being on the phone with your biggest customer who just happens to be in need of replacement units for their primary server. The inventory shows no units currently in stock and several units on back-order, when in fact the units are sitting on the shelf in the warehouse and available to be shipped the same day. You just lost a sale due to the fact that someone was manipulating the figures in a raw database file, they happened to find on the server in a mysteriously open area. What happens when the customer finds out that the equipment was really on the shelf in the warehouse? Or better yet, the vice president is giving a presentation to a large potential customer getting ready to sign a multi-million dollar deal for the flagship line of brand new multiple array disks enclosures and his laptop starts doing weird things and then suddenly the screen goes bright blue and white. Does anyone know or care what the message and all these numbers are on the screen? After trying to reboot, it is determined that the laptop will not boot. After giving it to the IT Group, they determine that it was struck with a computer virus that had a timed payload and just reformatted the hard drive. They report the findings to the VP and question whether a backup of the presentation was made. We all know the all too common answer to questions like those. "I was in a rush and put some things together for the presentation, but didn't get a change to put a copy on the server." Therefore no backup and no restore, so they will have plenty of time to practice using the

presentation software, because they will get to do it all over again and what happened to that multi-million dollar deal?

Potential for Damage

The potential for damage would have to be ranked extremely high. It can happen to anyone, at anytime, while at the office, traveling on a sales trip, or giving a presentation. This could be someone at GE's main office just as fast as it could be you or me.

Likelihood of Exploit

GE's systems are all run on the Windows 2000 operating system and are therefore potential targets to mischievous attack. According to the authors of Hacking Exposed, "…Out of the box, NT is configured to give away just about any piece of information a hacker would desire, and then some. Whether you consider this a design flaw or a capitulation to ease-of-use is irrelevant; these features exist and if you don't take steps to remedy them, someone can collect enough information about your NT network to mount a successful attack."[2] Since Windows 2000 is based on the Windows NT platform some of this can be taken for face value and some it can be taken "with a grain of salt." Although GE's senior management realizes that no solution is 100 % effective, they have tasked the IT group with providing necessary tools to get the job done. GE's senior management prefers to error on the side of caution with the helpful assistance of the IT group.

Mitigation

The IT Group's recommendation for this potentially crippling concern utilizes the principles of Defense in Depth. Brian McKenney defines defense in depth as a "..strategy[that]combines the capabilities of people, operations, and security technologies to establish multiple layers of protection … the objective is to implement defenses at multiple locations so that critical enclave resources are protected and can continue to operate in the event that one or more defenses are circumvented".[3] The layers of protection that the IT group will implement are:

1. A Cisco 3600 series router capable of IP filtering,

---

[2] McClure, Stuart, Joel Scambray, George Kurtz. Hacking Exposed, Network Security Secrets & Solutions. Berkeley:Osborne/McGraw-Hill, 1999. 58.

[3] Morgan, Conrad. "A Survival Guide for Security Professionals". 20 March 2002.
URL: http://rr.sans.org/practice/survival.php (5 May 2002).
Original source: McKenney, Brian. "Defense in Depth"
URL: http://www.mitre.org/pubs/edge/february_01/mckenney.htm (5 May 2002).

2. A primary Watchguard firewall to protect the external servers; WWW, SMTP and DNS,
3. A secondary Watchguard firewall to protect the primary network segment,
4. A tertiary Watchguard firewall to protect the R&D network segment,
5. Anti-virus software on all servers and workstations,
6. Two levels of content scanning of e-mail attachments, one configured on all three Watchguard firewalls and content scanning software on both the external and internal mail server.

The IT group is also preparing its final proposal to GE's senior management to include Intrusion Detection Servers (IDS) on each network segment for detection, monitoring and verification purposes. The IT group feels that the addition of the servers would be an additional layer of protection to the previous layers as well as provide another method of detection and notification. The IDS servers can be utilized in a proactive method by identifying potential problems, containing them from propagating or doing the servers and workstations harm and optionally executing code to trigger a performed response to predictable situations.

Overall Vulnerability

Data corruption will always be a major concern of GE's senior management, however by addressing the problems, having a plan and educating their IT group, senior management believes that this can be turned into a proactive situation rather than a reactive one. The risks therefore become more acceptable to everyone.

Corruption of the Server Environment

Overview of Threat

Professionals in the computer industry have seen time and time again that when they receive servers out of the box, the servers are not configured based on security of the individual system, but based on availability and functionality to the user. Plug the system into the network, configure a network address and give it some life. This is where "hardening the operating system" begins to play a key part of administrators' nightmares. Without the assistance of 3rd party security consultants, 3rd party software tools, and all too numerous websites that not only explain what the problems are and how to exploit them, administrators would be waiting for that inevitable bomb to drop or other shoe to fall. But on the other hand, there are also numerous websites that publish best or acceptable practices which are more than enough to take that out of the box system and turn it into that reliable system that you can confidently attach to your network and sleep well at night.

Relevance to GIAC Enterprises

Since GE needs to support not only external but internal servers in order to provide enough processing power and redundancy to accommodate applications in its computer environment, these systems have to be extremely reliable. After all, GE's business depends upon the servers being able to do their jobs and be available when an employee needs information. Server downtime can have disastrous implications ranging from inaccessibility to data to losing a multi-million dollar customer account.

Potential for Damage

This would have to be qualified as a medium-high to high potential for damage. There always exists the possibility that someone or something could penetrate the external defenses of the network and cause damage to GE's external or internal servers. With proper configuration, monitoring of currently released industry standard notifications regarding vulnerabilities, proper procedures, testing and continual upgrades and patches, GE's IT group can mitigate the risk that the outside world will influence their servers.

Likelihood of Exploit

GE's IT Senior staff has a unique relationship with the engineers in the R&D group. This relationship affords the IT Senior staff the capability of utilizing the server resources of the R&D group as a testing environment for GE's production servers. Since both groups thrive on the existence of cutting edge technology, the IT Senior staff makes sure that the R&D servers are always backed up and easily restorable prior to applying

patches and upgrades to the R&D servers. This makes sure that the R&D servers are protected in the event that a patch or upgrade causes unexpected results. This also gives the R&D servers the most current operating systems, allowing for the R&D systems benchmarks to be current regarding operating systems software standards. Utilizing this unique testing environment benefits both groups, since the IT Senior staff does not have to purchase additional equipment to perform their testing and the R&D group always has current operating system software for their development. Most IT departments do not have this luxury of having readily available test equipment at their disposal. Although the possibility exists of server corruption, GE's IT group has a distinct advantage over other IT departments and GE's senior management applauds the cooperation between the IT group and R&D group for mitigating this risk in a timely manner.

Mitigation

The IT group can mitigate the corruption to the server environment by making sure that the following tasks and procedures are followed:

1. The IT Manager will provide direction to the IT Senior staff as to the requirements of the new server, configuration, purpose and end user requirements.
2. When receiving new servers "out of the box", most come with operating systems currently installed. Since the IT Senior staff is basically unsure of the configuration of the server, the IT Senior staff will reinstall the operating systems consistent with the Server: Installation Procedure.[4] This will happen without being connected to the primary network, it may be accomplished by attaching it to a "test" network or R&D network instead.
3. Consistent with the Server: Upgrade Procedure, the IT Senior staff will upgrade and patch the operating system with solutions from the operating system manufacturer making sure that the Server: Upgrade Procedure is kept current. Notification will be made to the IT Security Officer (ITSO) and IT Manager of procedural changes.
4. The IT Senior staff will make modifications to the included operating system files as stated in the Server: Hardening Operating System Procedure. Notification will be made to the ITSO and IT Manager of procedural changes.
5. The IT Senior staff will install any and all applicable software based on the IT Manager's directions according to the Server: 3rd Party Software Installation Policy and Server: 3rd Party Software Installation Procedure. Notification will be made to the ITSO and IT Manager of procedural changes.
6. The IT Senior staff will configure end user access according to the IT Manager's direction and end user manager's directions.
7. The IT Senior staff will verify all configuration issues have been taken care of based on the Server: Configuration Checklist Procedure. Notification will be made to the ITSO and IT Manager of procedural changes.

4 Suggestion from article Spitzner, Lance. "Preparing NT for a firewall." Armoring NT. 16 April 2000. URL: http://www.enteract.com/~lspitz/nt.html (5 May 2002)

8. The IT Senior staff will place the new server on the appropriate network segment, configuring it properly with its given IP address. At this point the IT Senior staff will test all connectivity issues and adjust accordingly.
9. The IT Senior staff will reconfigure the router access list and all appropriate firewall configurations based on the IT Manager's requirements for end user access. The IT Senior staff will then test all given situations from all network segments to verify correct configuration, making sure to solicit the assistance from the end users that require access to any given application on the new server.
10. The IT Senior staff will then turn over the new server to the IT Administration group according to the IT: Server Administration Turnover Procedure. Notification will be made to the ITSO and IT Manager of procedural changes.
11. The IT Senior staff will then review all procedures and checklists and make adjustments accordingly. Notification will be made to the ITSO and IT Manager of procedural changes.

Overall Vulnerability

GE's senior management as well as their IT group realize that while Windows 2000 operating system is the current target of choice of most persons that want access to someone else's information, the policies and procedures that GE currently has in place and constant review and revision process will provide GE's network servers the most protection from malicious sources. The risk of having a server compromised always exists from external and / or internal sources but paying attention to the details in this circumstance will provide exponential rewards.

Evaluate and Develop Security Policy

Model Data Backup Policy

The text of this Backup Policy has been taken from Arizona State University West's website located at http://www.west.asu.edu/itweb/policies/UnivData/DataBackup.htm. This policy is being utilized strictly as an educational requirement of this practical. It is not the intention of this author to criticize nor ridicule the owners of this policy but to critique and analyze the policy according to SANS GISO course teachings and to rewrite this same policy with those teachings in mind. Since manufacturing companies are hesitant in displaying this type of information on their corporate websites, this policy is substituted in this training exercise for the requirement. This author wishes to thank Arizona State University for making this information publicly available with the hopes that everyone can utilize this information and learn from ASU's and SANS' insights.

```
ASU Computer System Backup Policy


      The purpose of this policy is to define the need for performing
periodic computer system backups to ensure administrative applications
software and university data are adequately preserved and protected
from destruction.

Approved by the Information Technology Advisory Committee (university
wide): 4/2/93.
Approved by the Main Campus Senior Vice President and Provost: 5/18/93.

Source:     Administrative Computing Advisory Committee.

Applicability: This policy applies to all units operating category A
            and B administrative applications as defined below and is
            strongly recommended for all computer users.

Background: Data can be destroyed by system malfunction or accidental
            or intentional means. Adequate backups will allow data to
            be readily recovered as necessary. The ongoing availability
            of university data is critical to the operation of the
            institution. In order to minimize any potential loss or
            corruption of this data, units responsible for providing
            and operating category A and B administrative applications
            need to ensure data is adequately backed up by establishing
            and following an appropriate system backup procedure.

Keywords:   Computer system backup, backups, retention, university
            data.

Policy:     Each unit responsible for providing and operating category
            A and B administrative applications must perform a system
```

backup on a periodic basis. The frequency of these backups, retention location, and the retention timeframes for each will be dependent on the criticality and volatility of the data residing on each system.

Guidelines: Computer systems that create or update university data on a daily basis need to be backed up on a daily basis to minimize the exposure to loss of critical data.
It may be useful to establish a hierarchy of backup cycles. For instance, a daily backup cycle might involve retaining seven sets of backups (one week). Then the seventh daily backup is retained for a longer period, say one month, as part of a weekly backup cycle. Finally, the fourth weekly backup might be retained for one year as part of a monthly backup cycle. In this way, the risk of catastrophic loss is minimized at a reasonable media cost.

Definitions: TISC ADMINISTRATIVE APPLICATION TYPES -
A - Applications which collect and/or update university data.
B - Applications which use university data for "official" purposes outside of the local unity, but which do not collect and/or update university data.
C - All other applications: those which deal with data for local purposes only.
UNIVERSITY DATA - (AKA Administrative Data/Information) is the collection of data elements which are relevant to the operations, plans, or management of more than one ASU unit or are reported on or used in "official" administrative university reports.
SYSTEM BACKUP - a documented procedure for copying applications software and data files that reside on computer disks to a portable medium (such as tape or diskette) or to a medium that is physically remote from the originating system.

Consequence of Non-Compliance: Non-compliance with this policy could severely impact the operation of the institution by exposing the University to permanent loss of university data, loss of state funding and federal funding. It may also expose the individual or the University to legal action.

Evaluation of Data Backup Policy

The ASU Computer System Backup Policy is well written and covers the major issues that need to be included in a document of such nature. The issues included in the policy consist of:

Purpose statement at the beginning of the document stating why the policy is being established and the issue at risk being to "ensure administrative applications software and university data are adequately preserved and protected from destruction."[5]

Background statement included to expand upon the purpose statement and provide additional reasoning for following through on implementation of this policy.

Scope statement is actually included in the background statement in the form of "In order to minimize any potential loss or corruption of this data, units responsible for providing and operating category A and B administrative applications need to ensure data is adequately backed up by establishing and following an appropriate system backup procedure."[6]

Policy statement is short and concise. However, leaving the frequency, retention and retention time frames of the backups to the end user should require a definition in time frames that is stricter, leaving no room for misinterpretation.

Responsibility statement is not specifically stated in this document. It is given that the source was the Administrative Computing Advisory Committee and was approved by the committee as well as the Main Campus Senior Vice President and Provost. It does not clearly state who is responsible for the policy as well as information on who can review, approve or modify the policy. Also missing from this section is how often the policy will be reviewed. This item is not required in the policy document and may have been omitted by the committee for purposes of publishing this document on their publicly available website. Sometimes when information is made available on publicly accessible websites, organizations choose to omit information that they feel may be "proprietary" or "confidential" in nature.

Action statement is actually a combination of the Policy and Guidelines sections of this policy. The action statement should define what specific actions are necessary and when they should be accomplished. In this policy, the backups should be performed on a daily basis. The inclusion of the example of rotating tapes to daily, weekly and monthly is an

---

[5] "ASU Computer System Backup Policy". 12 April 2001. Arizona Board of Regents. URL: http://www.west.asu.edu/itweb/policies/UnivData/DataBackup.htm (5 May 2002)
[6] "ASU Computer System Backup Policy". 12 April 2001. Arizona Board of Regents. URL: http://www.west.asu.edu/itweb/policies/UnivData/DataBackup.htm (5 May 2002)

absolutely essential portion of the policy document and this policy does a great job of keeping the information at a very basic detail so as to not confuse the end users of the document.

Overall the policy does an extremely good job of keeping the information detail to a readable content for the end users. However the clarity of some details could become misleading to the end users if not actually spelled out for them.

Revised Data Backup Policy

For purposes of this exercise, the author has taken the preceding information and revised it according to a manufacturing company rather than an educational institution. The educational policy was clearly necessary for the individual workstation level of the institution while the corporate policy will reflect that of a server environment.

DATA BACKUP POLICY (REVISED)

Purpose

The purpose of this policy is to define the process of data storage for the protection and integrity of GIAC Enterprises' (GE) primary servers regarding backup and recovery of the same information.

Background

It is commonly held that computer systems will fail, it is not a matter of why or how, but a matter of when. Several external factors, of which GE is not in control can cause occasional or severe problems to their servers; natural disasters such as flood, tornadoes or lightning to man-made disasters such as trucks hitting a major power poll outside GE's office and disturbing the power for a prolonged period of time. GE's most important assets are their R&D schematics, drawings, specifications and processes, along with their patents and proprietary trade secrets, which must be saved at all costs. Loss of this information could cause severe downtime resulting in: lost production, delay of product, wasted time in recreation effort, deterioration in customer relationships, loss of market share and inevitably loss in income.

Scope

This policy pertains to all primary servers contained in GE's main office. It includes all files related to the operating system, installed applications and data pertaining to those applications.

Policy Statement

Backups of all primary servers are run nightly, after business hours, to make sure that all files are closed and available for backup. Full backups are done on all primary servers each night, Monday through Friday. Incremental backups are permissible on systems that require large amounts of data be backed up in a single evening. Full backups are done weekly. At the end of the month, full backups are done to a separate series of tapes and labeled with "End of *month, year*". At the end of the year, full backups are done to another separate series of tapes and labeled with "End of *year"*. Backups are to be complete prior to beginning of next business day, currently defined in the GE Attendance Policy as being 7 AM.

Responsibility

The IT Manager is responsible for setting backup schedules, changing removable tapes, monitoring the success / failure of each system's previous nightly backup, rerunning the backup procedure if required and time permits between server checks and next available backup schedule, logging the backup results in the yearly tape backup document and storing the backup tapes according to daily, weekly, monthly, and yearly. The IT Manager is also responsible for data restores to misplaced data files at the individual request of the person that owns the original data files needing to be recovered. The person or persons responsible for this activity in the absence of the IT Manager will be an appointed member of the IT Staff at the request of the IT Manager.

The IT Security Officer (ITSO) audits this policy on a monthly basis for compliance and make appropriate recommendations to the IT Manager regarding such compliance issues as deemed necessary.

Actions

The daily, weekly, monthly and yearly tapes are backed up onto appropriate media (either 4mm or DLT based on system configuration). Daily tapes are stored on a rotational basis to include enough tapes for each system for a period of 31 days. Weekly tapes are stored on a rotational basis to include enough tapes for each system for a period of 5 weeks. Monthly tapes are stored on a rotational basis to include enough tapes for each system for a period of 12 months. Yearly tapes are stored on a rotational basis to include enough tapes for each system for a period of 10 years. This is due to a combination of acceptable risks from GE's senior management that have been determined either based on engineering, financial or individual department requirements. No data will be recovered after it has aged more than 10 years time. GE's senior management also realizes that there are time gaps where data might not be available due to rotation of tape series and / or no detail being available after the second yearly rotation of tapes to provide sufficient detail on a daily, weekly or monthly basis. Media retention

period for all applicable media is marked on the media labels with a date two years time from the first date of use. Once this date has expired, media is to be given to the IT Manager for proper disposal according to the IT: Proper Media Disposal Procedure to insure that corporate information is not available outside of GE's corporate structure.

All media from all primary system backups is to be stored in the appropriate labeled FireKing ™ file cabinet and corresponding FireKing Media Vault™[7] located in the IT Server Center. This safeguard not only provides fireproof storage for the backup media, but also provides availability of media for restorable purposes.

DEVELOP SECURITY PROCEDURES

DATA BACKUP PROCEDURE

Purpose

The purpose of this Data Backup Procedure is to provide definition to GIAC Enterprises' (GE) Data Backup Policy. All previous copies of this procedure are to be destroyed and printed copy is only for reference by the authorized person(s) performing the designated tasks.

Requirements to Perform Tasks

The only employees assigned the tasks of data backup / recovery of data contained on GE's corporate servers are the IT Manager, IT Senior staff and IT Administration staff.

Prerequisites that are required for performing these tasks are:
1. Authorized physical access to IT server rooms,
2. Authorized access to Administrator account on all servers performing backups,
3. Authorized access to the Veritas Backup Exec™ software for Windows NT,
4. Knowledge of backup software, schedules, media used and physical storage requirements,
5. Physical access and keys to fireproof cabinets and vaults utilized in physical storage of media.

Responsibilities

Backups of all primary servers are run nightly, after business hours, to make sure that all files are closed and available for backup. Full backups are done on all primary

[7] FireKing ™ and FireKing Media Vault™ are authorized trademarks of FireKing International – http://www.fireking.com

servers each night, Monday through Friday. Incremental backups are permissible on systems that require large amounts of data be backed up in a single evening. Full backups are done weekly. At the end of the month, full backups are done to a separate series of tapes and labeled with "End of *month, year*". At the end of the year, full backups are done to another separate series of tapes and labeled with "End of *year"*. Backups are to be complete prior to beginning of next business day, currently defined in the GE Attendance Policy as being 7 AM.

The IT Manager is responsible for setting backup schedules, changing removable tapes, monitoring the success / failure of each system's previous nightly backup, rerunning the backup procedure if required and time permits between server checks and next available backup schedule, logging the backup results in the yearly tape backup document and storing the backup tapes according to daily, weekly, monthly, and yearly. The IT Manager is also responsible for data restores to misplaced data files at the individual request of the person that owns the original data files needing to be recovered. This request will be in the form of an e-mail sent from the owner of the data wishing to be recovered sent to the IT Help Desk e-mail account for purposes of tracking and accountability. The person or persons responsible for this activity in the absence of the IT Manager will be an appointed member of the IT Staff at the request of the IT Manager.

Backup Process

All backup jobs have been scheduled by the IT Manager to commence at 18:30 daily on all servers. This allows adequate time for all employees to log off of their respective workstations so that all files located on the servers are closed and ready for backup. All jobs are setup in such a manner as to include all drives located on the server regardless of operating system or data volumes. All jobs are setup to include tape rewrite option, full backup (unless designated by IT Manager to provide incremental backup capability), the name of the server included in the tape label as "GE *Server* FULL *YYMMDD"* (where two digits represent the year, month and date of backup), default media set, verify after backup complete, compression set to Hardware (if available, otherwise software), backup open files set to yes.

Daily Backup Verification

1. Log onto appropriate server as Administrator from the server console
2. Open the Seagate Backup Exec icon
3. Respond OK to Media Information message from previous nightly backup
4. Open Job Monitor tab
5. Check for "successful" Job Status for the previous night's backup
6. If the Job Status is anything other than "successful", double-click entry
7. Click Log File tab and review for errors

8. If necessary, open the operating system's Event Viewer and check Log > System for hardware error to verify existing problem with tape backup job
9. Eject current tape(s), run cleaning tape for drive(s)
10. Rerun tape backup with another blank tape(s) (preferably brand new tape(s)) providing that time permits based on previous timed successful completions of same tape backup job
11. If time does not permit, yearly tape log will have to be marked "BAD-*initials"* and the tape(s) marked bad on the tape label so that it can be replaced the next time it is to be utilized in the tape rotation
12. Close Backup Exec software
13. Eject tape(s) from tape drive(s)
14. Reload tape(s) based on daily, weekly, monthly or yearly tape rotations
15. Record status as "OK-*initials*" in the yearly tape backup document for the appropriate date of the previous tape backup
16. Store the tape(s) in the appropriate FireKing™ cabinet and FireKing Media Vault™ [8]according to the whether the tape(s) belongs in the vaults for daily, weekly, monthly or yearly tapes.
17. Perform same procedure on all GE servers making sure to log off of each successive server environment. Policy is given in the IT: Secure Server Environment Policy that does not permit any authorized person to leave a server signed onto the Administrator account on any of GE's corporate servers.

Audit Verification

The IT Manager performs data recovery on a monthly basis according to the IT: Server Data Recovery Procedure provided that time and system resources are available. This will require coordination with the R&D group, as most of their systems serve as "test" environments for GE's production systems.

The IT Security Officer (ITSO) audits this policy on a monthly basis for compliance and makes appropriate recommendations to the IT Manager regarding such compliance issues as deemed necessary.

Addendum

This procedure covers the data backup of GE's corporate servers. Workstation data backup is covered in a separate policy and procedure entitled GE: Workstation Data Backup Policy and GE: Workstation Data Backup Procedure.

[8] FireKing ™ and FireKing Media Vault™ are authorized trademarks of FireKing International – http://www.fireking.com

References

McClure, Stuart, Joel Scambray, George Kurtz. Hacking Exposed, Network Security Secrets & Solutions. Berkeley:Osborne/McGraw-Hill, 1999. 58.

Morgan, Conrad. "A Survival Guide for Security Professionals". 20 March 2002. URL: http://rr.sans.org/practice/survival.php (5 May 2002).

McKenney, Brian. "Defense in Depth" URL: http://www.mitre.org/pubs/edge/february_01/mckenney.htm (5 May 2002).

Spitzner, Lance. "Preparing NT for a firewall." Armoring NT. 16 April 2000. URL: http://www.enteract.com/~lspitz/nt.html (5 May 2002).

"ASU Computer System Backup Policy". 12 April 2001. Arizona Board of Regents. URL: http://www.west.asu.edu/itweb/policies/UnivData/DataBackup.htm (5 May 2002)

FireKing International. URL: http://www.fireking.com (5 May 2002)

Additional References

Cisco 3600 series router. URL: http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm (5 May 2002)

Winters, Scott. "Securing the Perimeter with Cisco IOS 12 Routers". 15 August 2002. URL: http://rr.sans.org/firewall/blocking_cisco.php (5 May 2002)

Cisco Technical Documents. URL: http://www.cisco.com/univercd/home/home.htm (5 May 2002)

Watchguard Technologies, Inc. Firebox Solutions. URL: http://www.watchguard.com/products/wgls.asp (5 May 2002)

Compaq Proliant DL580. URL: http://www.compaq.com/products/servers/platforms/index.html (5 May 2002)

Microsoft IIS 5.0. URL: http://www.microsoft.com/windows2000/server (5 May 2002)

Microsoft Exchange 5.5 SP4 URL: http://www.microsoft.com/catalog/display.asp?subid=22&site=599&x=40&y=12 (5 May 2002)

Microsoft SQL 7.0
URL: http://www.microsoft.com/SQL/evaluation/70/default.asp (5 May 2002)

MetaInfo's MetaIP DNS.
URL: http://www.checkpoint.com/products/management/metaip.html (5 May 2002)

HP Laser Printers.
URL: http://welcome.hp.com/country/us/eng/prodserv.htm (5 May 2002)

Compaq EVO 500 Workstation.
URL: http://www.compaq.com/products/desktops/index.html (5 May 2002)

Compaq EVO N600C Laptop.
URL: http://www.compaq.com/products/notebooks/ (5 May 2002)

APC UPS Solutions.
URL: http://www.apcc.com (5 May 2002)

SANS Reading Room Documents.
URL: http://rr.sans.org/index.php (5 May 2002)