GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

Information Security Officer
GISO Practical Assignment
Version 1.2

© SANS Institute 2000 - 2002, Author retains full rights.

GIAC ENTERPRISES

Security Risk Analysis, Policies and Procedures

Submitted by: Mulu Alem Syoum
14 August 2002

Table of Contents

© SANS Institute 2000 - 2002, Author retains full rights.

ASSIGNMENT 1 — DESCRIBE GIAC ENTERPRISES

Description of GIAC Organization

GIAC is the Secretariat of an Executive Committee of an international non-profit organization that engages in environmental protection. The organization assist developing countries in phasing out ozone depleting substances by receiving funding from industrialized countries.

The Executive Committee comprises seven members, each from developing countries and industrialized countries. The functions of the Committee include the development of operational policies, criteria for project eligibility, and other guidelines and administrative arrangements, monitoring of the implementation of these policies, approval of implementing agencies' business plans and work programmes, approval of expenditures for investment projects and other activities, allocation and disbursement of resources, and the monitoring and evaluation of performance. The Executive Committee holds three meetings per year.

GIAC assists the Committee in the discharge of its functions. Its activities include: development of the three-year plan and budget and a system for fund disbursement; management of the business planning cycle; monitoring the expenditures and activities of the implementing agencies; preparation of policy papers and other documents; review and assessment of investment projects, country programmes and the business plans and work programmes of the implementing agencies; liaison between the Committee, governments and implementing agencies; and servicing meetings of the Executive Committee. GIAC partners with other implementing agencies and government agencies involved in similar work, for example, national ozone units.

IT Infrastructure

GIAC's technology infrastructure is defined by the internal and interface elements of the network and the attached devices that include the server computers, routers and firewalls, specialized storage devices and other elements. GIAC's network/device infrastructure is subdivided by firewalls into zones - logically and physically defined areas with similar protective needs or access characteristics.

The IT infrastructure that supports the enterprises' business activities is composed of the following major elements and technologies:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Device	Hardware	Software
Router	Cisco 1600-AC	12.0
Firewall	Cisco Pix 515	6.2
VPN	Cisco Pix 515	6.2
Web/SSL Server	HP Netserver LH3000	Windows 2000/IIS 5.1
Mail Server	HP Netserver LH3000	Windows 2000/Imail 7.2 (IPSwitch)
File Server	HP Netserver LH3000	Novell 5.1
Database Server	HP Netserver LH3000	Windows 2000/SQL Server 2000

The highest priority application components include: File Server, Web Server, GIAC SQL Database and Mail Server. The File Server contains all the project proposals that submitted by all the Article 5 countries through their ozone units or implementing agencies, as well as country programme data. The Web Server contains the public site where the reports of the Executive Committee Meetings can be retrieved. The secured site of the Web Server retrieved information from the secured SQL database and the project proposals submitted by countries. The Mail Server is where countries, implementing agencies, members of Executive Committee and national ozone units communicate electronically with GIAC and where GIAC corresponds back on a timely manner, especially in order to meet the submission deadlines of upcoming meetings. It is the top priority to ensure the mail server runs 24 hours without any disruption.

Workstation and Network equipment and applications

GIAC has approximately 30 desktop PC's using Windows 95\98\2000\XP (with all patches) as its operating system. The systems have only required services enabled. GIAC's applications include word processing, database, spreadsheet file storage, printing services, internal e-mail and servers, data storage facilities and anti-virus software.

Internal Servers

One HP Netserver LH 3000 Raid 5 configuration with Novell server 5.1, and five HP Netserver LH 3000 Raid 5 configuration with Windows 2000 (with all patches) as their operating system (for SQL Server, Web Server and Back-up Server). These systems have only required services enabled, have at least two NICs (one connecting to Administration Maintenance Security Console), have logging turn on, run anti-virus software and are backed-up regularly. Novell and Microsoft Windows 2000 are used primarily to host Microsoft based productivity applications such as Office, Outlook, and Mail services. TCP/IP is implemented throughout the organization, supported on an Ethernet backbone. All client computers are, at least, Windows 95 or greater.

The internal network is connected to the external network in a restricted manner through the interface zone and through the use of the VPN technology.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Router

GIAC's Gateway will have published IP address.

GIAC is connected to Internet Service Providers (ISP), T1 line. The router will also allow GIAC to filter out network attacks such as IP spoofing and DOS attacks. Furthermore, the router will be used to control the packets allowed to enter the demilitarized zone (DMZ). Accepted packets will proceed to a Cisco Pix 515 Firewall, which will forward packets to either the external/internal server (on DMZ 1), external SMTP server (on DMZ 2), or to the client from whom the information was requested (HTTP).

Firewall and VPN Network DMZ

After the router, the second layer is a firewall. In GIAC's network, the VPN software will provide VPN connections between GIAC and to GIAC's partners. The first system in the VPN DMZ is the firewall, which only allows in-bound VPN connections made directly to the VPN Application Server. No other connections are allowed. All communication from inside and/or outside remote, the VPN server is encrypted.

Mail Server

SMTP traffic exchange will only be allowed between the external and internal SMTP servers. In the same manner, in the PIX 515 is DMZ, providing gateway services for in-and-outbound SMTP email, and outbound web connections for all users. Any inbound traffic passing through this SMTP server is automatically scanned for viruses, and other harmful or inappropriate content. This subnet is connected to the Internet via a CheckPoint Firewall, which also protects the main DMZ.

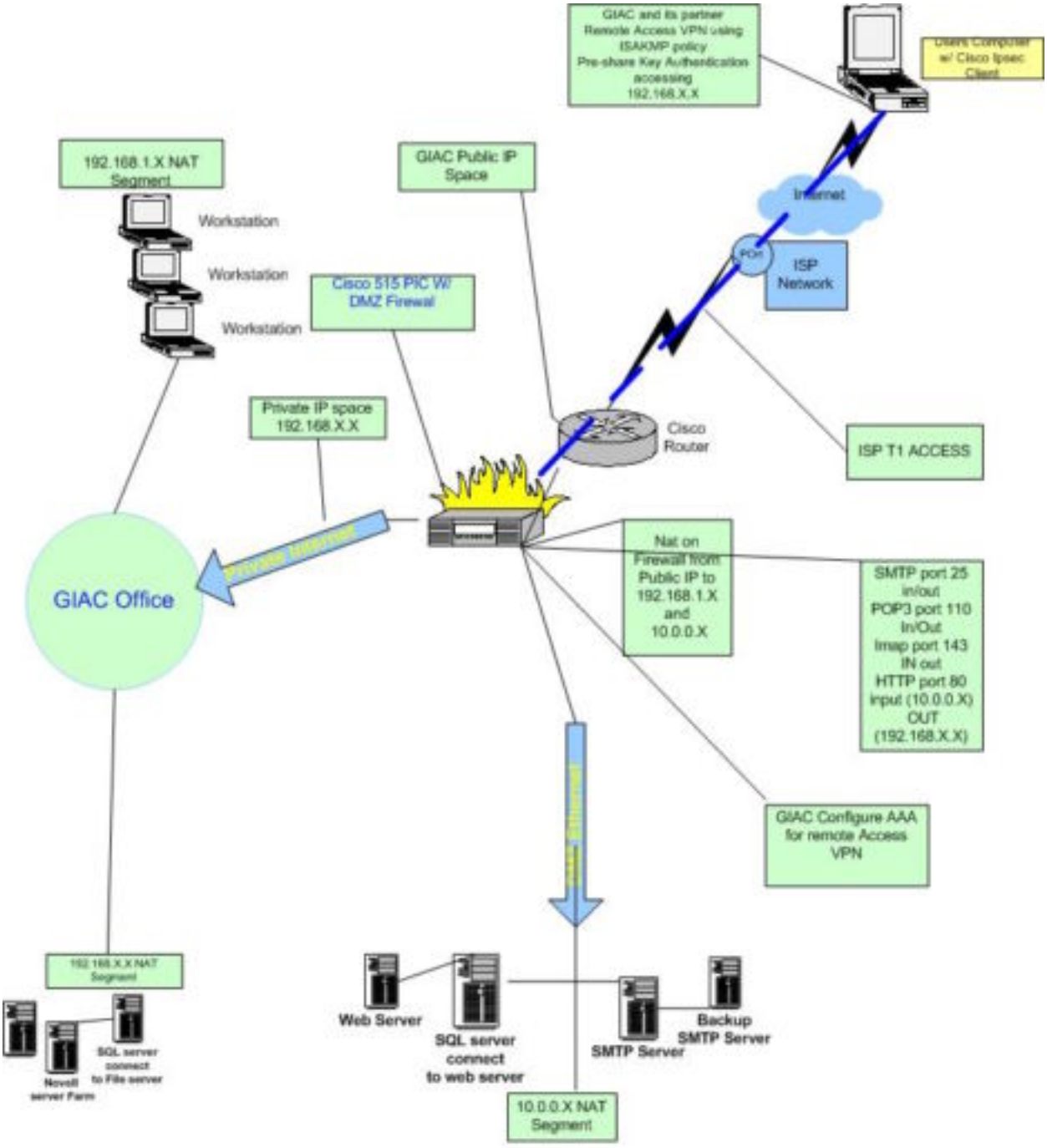
Web Server

Web services are handled by Microsoft IIS 5.0. All web applications that access to confidential or sensitive information are constructed using an Internet access to confidential information which is protected through SSL sessions and password authenticated. For all protected documents on the web, session states are managed by the web application server through the use of non-permanent cookies.

© SANS Institute 2000 - 2002, Author retains full rights.

Network Diagram

Basic GIAC's network diagram is shown as follow:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Business Operations

GIAC, in spite of a non-profit organization, has a high number of business operations that need to be performed. Starting from countries submitting project proposals with ozone depleting substances (ODS) consumption and production data, information on ODS plants; GIAC evaluating countries' data, communicating with implementing agencies and national ozone units comments and recommendations; countries amending their submissions; GIAC submitting the amended submissions to the Executive Committee, Executive Committee approving the projects and deciding on the funding levels, implementing agencies carrying out the project and GIAC monitoring and evaluating the project by collecting data from national ozone units, making sure the countries are in compliance and follow agreements. The following describes the business operational of IT needs for GIAC, its partners and its employees in order to fulfil its mission. For ease of understanding, the primary operational IT requirements are summarized as follows:

Service	Direction	Executive Committee Members	Implement-ing Agencies	National Ozone Units	Employees	Remote Users
Web	Inbound	X	X	X	X	X
	Outbound	X	X	X	X	X
SSL	Inbound	X	X	X	X	X
	Outbound	X	X	X	X	X
Email SMTP	Inbound	X	X	X	X	X
	Outbound	X	X	X	X	X
VPN	Inbound	X	X	X	X	X
	Outbound		X	X	X	X
Database (SQL)	Inbound		X	X	X	X
	Outbound				X	X

In GIAC IT infrastructure, there are five main groups of users, namely Executive Committee members, implementing agencies, national ozone units, employees and remote users. There are two directions: inbound and outbound. The inbound traffic connects and transmit from the internet to GIAC, and the outbound connects and transmit from GIAC to internet (partners).

Executive Committee Members

Executive Committee Members require access to the secure web site to download meeting documents which are limited to distribution. They must be able to contact GIAC by email for comments on documents. GIAC must provide Executive Committee members with web, Secure Socket Layer (SSL), and public email to meet these operational requirements. Executive Committee members reach these services via the Internet with SSL-enabled browsers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Implementing Agencies

The main role of implementing agencies are to assist national ozone units of Article 5 countries to prepare project proposals and ODS phase-out related activities which are reviewed by GIAC and considered by the Executive Committee. Implementing agencies deal with a lot of sensitive data, for example, country consumption data and funding. They must be able to contact GIAC by email for comments on documents. GIAC must provide implementing agencies with web, Secure Socket Layer (SSL) and public email to meet these operational requirements. Implementing agencies can reach these services via the Internet with SSL-enabled browsers.

National Ozone Units

National ozone units need to report to GIAC and implementing agencies sensitive country consumption data of ozone depleting substances over internet and email in order for GIAC to determine funding available for the country concerned. These users need to access SSL, VPN with VPN software using pre-shared key to GIAC, and SQL.

Employees

Employees require access to Internet, corporate email, and corporate servers and applications. In addition, employees need to access SSL, Virtual Private Network (VPN) to web server and LAN File server. Employees reach these services via GIAC IT infrastructure.

Remote Users

On a remote usage, GIAC realize that there is a bottleneck of a bandwidth usage of a T1 line. Therefore, the remote users should be limited to only staff members who travels (access permitted only during the travel time) and partners (selected focal point contact per agency). However, GIAC is reviewing the budget to upgrade the T1 line to a T3 line. Remote users require access to Internet, corporate email, public email, and corporate servers and applications through Virtual Private Network (VPN) facility.

© SANS Institute 2000 - 2002 Author retains full rights.

Assignment 2 - Identify Risks

The purpose of this section is to identify the three most critical areas of risk to GIAC Enterprises. Although many risks may exist, dealing with the three largest risks will do the most to ensure the continued business operations of GIAC Enterprises.

Security Risk 1 – Internal LAN

Description of the risk

The internal Secure LAN contains GIAC's most important resources for its daily operations. Unauthorized access to resources on this network could have the following impact on GIAC:

- Since countries data are very sensitive, if GIAC employees were able to access information on the network that they were not authorized to, they may be able to inappropriately manipulate the data for personal gain.

- Theft of sensitive data, which could impact GIAC's position between countries, implementing agencies and national ozone units if certain information were made publicly available.

- Unacceptable interruption, such as delays in project approvals, could occur if important data or software was compromised.

- Countries' confidence in GIAC would be damaged if their data were accessed by unapproved sources from GIAC's network.

The threat to the LAN server is from two main sources, two different courses of action are recommended to mitigate the risk.

Insiders

The most likely type of unauthorized access to resources within the GIAC network is by internal GIAC employees. These employees may or may not be attempting to access this information with malicious intent.

Outsiders

Since the data is very sensitive, there is a good possibility that external individuals who are not affiliated with GIAC may try to access GIAC's network resources for personal gain.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Mitigating Steps

Insiders

- Install anti-virus software and automated update in the file server and all workstations.
- Implement a VLAN scheme to isolate the LAN server.
- Use one server for sensitive recipe information and another for the general internal company related material.
- Implement and enforce a strong password policy.
- Implement a RADIUS server to track authentication, authorization and accounting (AAA) for the LAN server.
- Make specific reference to the information on the LAN server in the Acceptable Use Policy.
- Ensure the LAN server is protected by appropriate physical security.

Outsiders

To prevent attacks from outsiders, the following steps need to be taken:

- All traffic coming from remote to GIAC (internal LAN) must first be authenticated though the VPN DMZ.
- Move the Mail Relay server from the inside subnet to the DMZ.
- Implement a VLAN scheme to isolate the LAN servers located there.
- Implement an Intrusion Detection System. Locate it on the inside LAN, and place a sensor in the DMZ.
- Ensure that the server OS is hardened. There does not appear to be a coherent policy of ensuring that servers are running the most current patch level.

Security Risk 2 – Virus Attack on GIAC's Network

Description of the risk

The risk to GIAC from a malicious software attack is very high. If a virus, worm, trojan or other maliciously created piece of software were to get onto the GIAC network, business operations could be seriously impacted. Examples of the potential impact to GIAC's business are shown below:

- A worm could be used to install an agent on the GIAC network that could be used to launch a coordinated attack against other networks. This would leave GIAC potentially liable for any damage caused to the external organization.
- If a resource-intensive worm were to penetrate GIAC's network, it could reduce available network bandwidth and possibly make network resources inaccessible. GIAC's operations would be impacted and delays will occur.

© SANS Institute 2000 - 2002, Author retains full rights.

- GIAC's image could be negatively impacted if governments/organizations received virus-infected files.

Unfortunately, due to the prevalence of viruses, the likelihood of a virus or worm attempting to infect GIAC's network resources is very high.

Mitigating Steps

To mitigate the risk of GIAC's network becoming infected with malicious software, the following steps have been taken:

User Training and Awareness

New company employees are required to attend an orientation session during the first week of employment with GIAC. This session contains information about GIAC's expectations regarding information security and includes specific actions that individuals should take to protect themselves and GIAC's systems from computer viruses and malicious code.

Anti-Virus Software

All PCs that connect to the GIAC network are required to use up-to-date anti-virus software. To enforce this, a central anti-virus update is provided to ALL workstations and servers. This central anti-virus update will check automatically twice a day and will retrieve the latest definition file. The central anti-virus will then update the latest file to all the workstations and servers. Since network administrators receive alert messages from the software vendors and have latest information on new virus risks, for any useful events, administrator will take action accordingly. This will ensures that all workstations and server are protected.

Anti-Virus software on mail server

Anti-Virus software is integrated on the mail server itself for added protection. All incoming email will be checked for virus thus prevent virus from being received in the workstation. GIAC also implements content filtering on the e-mail gateway system to prevent SPAM. To further reduce the likelihood that an individual will receive an infected e-mail message, certain executable-type attachments are not allowed to be sent via e-mail. The integrated anti-virus software to the mail server will automatically update definition file as soon as they have been made available from the vendor.

Anti-Virus Software on File Servers

GIAC uses anti-virus software on all internal file servers which contain Windows or Macintosh files. The software is configured to run in a real-time mode and is also scheduled to perform a full system scan on a daily basis. The automated central virus

© SANS Institute 2000 - 2002, Author retains full rights.

software will update definition file as soon as they have been made available from the vendor.

Security Risk 3 – Disaster Recovery/Business Continuity

Description of the risk

Data and information of countries is the "crown jewel" of GIAC. The systems and network infrastructure that stores, processes and provides access to countries data and information, such as consumption and production data of ozone depleting substances, ozone depleting substances producing plant information and funding requested and approved must be protected at all costs. In order to ensure business continuity, insuring the 24/7 operation of systems is top priority.

The centralized location of the core systems of the GIAC file server and database server increases the vulnerability to the risk of damage due to a disaster. The core host systems provide a repository of countries data. The availability of the information is the main concern. Executive Committee requires this information from GIAC on a scheduled basis in order to approve project requested during Executive Committee meetings. Unavailability of a small portion of this information could result in delaying the preparation of documents for the Executive Committee Meeting, delaying phase out of ozone depleting substances and wrong calculation of project costs, creating conflicts between countries and thus lose funding from bilateral agencies. Finally GIAC requires quick, accurate and current information to expedite approvals of projects. Unavailability of the core systems and the related data would negatively impact operations in the following ways:

- Legal and regulatory consequences, and financial consequences resulting in loss of bilateral agencies funding.
- Slow down in the phase-out process of ODS.
- Slow down in the preparation and evaluation of the country project proposal.
- Interruption of hosting of Executive Committee meetings, which includes registration of delegations and posting meeting documents on line etc.

Mitigation Steps

The following measures must be taken to ensure data and systems availability against the risk of a disaster:

- Develop a disaster recovery plan including procedures – a detailed disaster recovery plan should be easily understood, so staff could easily follow. A good disaster plan will enable fast recovery and ensure data availability and business continuity.
- Provide a backup system for the primary server – When the primary server goes down, the back up system will automatically goes up. Since the backup system

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

mirrors exactly the primary server, when the primary server is down, employees can continuously working at the backup system without any interruption. Furthermore, the IT staff can start immediately repair the primary server without any worries about lag time and distribution of business continunity.

- Contract for off-site storage of critical data – For example, weekly tape back up can be stored in a safety box outside the office premises. It is also possible to contract data storage company to store organization's critical data. Offsite storage of critical data ensures availability of data when disaster occurs and onsite data is no longer recoverable due to fatal loss or damage.
- Rotate backup tapes daily ensures up-to-date information is available at all times for restoration.
- Train IT staff and GIAC management on disaster recovery procedures – It is an important practice. When disaster arrives, IT staff and GIAC management can right away carry out recovery procedure to ensure that things can get back to normal in the shortest period.

© SANS Institute 2000 - 2002, Author retains full rights.

ASSIGNMENT 3 — EVALUATE AND DEVELOP SECURITY POLICY

The following policy was obtained from:
"http://www.west.asu.edu/itweb/policies/UnivData/DataBackup.htm"

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

© SANS Institute 2000 - 2002, Author retains full rights.

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.

(Copyright Arizona Board of Regents. Contact Information Technology. Updated Friday April 13 2001)

© SANS Institute 2000 - 2002, Author retains full rights.

Evaluation of ASU Computer System 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: The purpose statement is to state why the policy is being established and the issue at risk. In the ASU Computer System Backup Policy, the purpose is stated clearly at the beginning of the document as "ensure administrative applications software and university data are adequately preserved and protected from destruction[1]".

Background: The ASU Computer Systems Backup Policy has a clear written background statement. It provides additional reasoning on implementation of this policy and is an expansion of the purpose statement.

Scope: The section of scope statement is not stated individually in the ASU Computer Systems Backup Policy, but it is included in the background statement as "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"[2]. It is suggested that to extract this part from the background statement and to make a stand alone scope statement in order for clearness and ease of understanding.

Policy statement: The policy statement is concise and clearly states what need to be done. However, the frequency, retention location and retention time frames of the backups can be defined more precisely in order to prevent misinterpretation.

Responsibility: The responsible party or person is not specifically stated in this document. It is only indicated that the source of this policy was the Administrative Computing Advisory Committee and was approved by the Information Technology Advisory Committee, as well as the Main Campus Senior Vice President and Provost. We do not clearly know which party is responsible for the policy and have the rights to draft, approve and modify the policy. Also missing from this

[1] "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)
[2] "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)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

section is how often the policy will be reviewed. Although these items are not necessarily required in the policy document and may be purposely omitted because of publishing on publicly available website, it is better to include these items in order to have a clear, complete and informative policy and to contact the right person when necessary.

Action: The action statement defines what specific actions are necessary and when they should be accomplished. There is not such an action statement in this policy, instead specific actions need to be taken (the backups on computer systems that create or update university data) at specific time (daily basis) is mentioned in the policy and guidelines statement. The policy keeps the information at a very basic detail so end user can understand easily and avoid confusion. The inclusion of the example of establishing a hierarchy of backup cycles is a very useful portion of the policy document.

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

Revised Security Policy for GIAC

Source: IT Department

Purpose: The purpose of this policy is to define the process of data storage for the protection and integrity of GIAC primary servers regarding backup and recovery of the same information.

Background: It is quite common that computer systems will fail because of unspecified reasons. Several uncontrollable external factors can cause occasional or severe problems to their servers. GIAC's most important assets are the data and information of countries, such as consumption and production data of ozone depleting substances, ozone depleting substances producing plant information and funding requested and approved, which must be protected at all costs. Loss of this information could cause severe downtime resulting in: delaying phase out of ozone depleting substances and wrong calculation of project costs, creating conflicts between countries and loss of credibility and reducing funding from bilateral countries.

Scope: This policy pertains to all primary servers contained in GIAC's office. It includes all data files except the operating system, and installed applications.

© SANS Institute 2000 - 2002, Author retains full rights.

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 Thursday. Every Friday, a weekly full backup is done to a separate series of tapes and these tapes are deposited in a safety box outside the GIAC premises. At the end of the month, full backups are done to another separate series of tapes and labeled with "End of month".

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 and monthly. The IT Manager is also responsible for data recovery. The person responsible for this activity in the absence of the IT Manager will be an appointed member of the IT staff upon request of the IT Manager.

The ITSO manager will be responsible for auditing the policy on a monthly basis for compliance and make appropriate recommendations to the upper management. However, since GIAC is still in the process of appointing an ITSO, the IT Manager will temporarily take up the responsibility of ITSO in the organization.

Action: The daily, weekly and monthly 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. Backup media need to be properly labeled at all times so information can easily be located.

All daily media from all primary system backups is to be stored in fireproof and waterproof cabinet located in the office of the IT Manager in order to facilitate data recovery. All the weekly media will be contracted for off-site storage.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 4 — DEVELOP SECURITY PROCEDURES

Purpose

The purpose of this procedural document is to define how the security policy of GIAC be implemented. Only data backup is considered here.

Actions

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. 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*". Backups are to be complete prior to beginning of next business day, before 8 AM.

Responsibilities

IT Manager is fully responsible for the backup, verification and data recovery procedures.

Process

All backup jobs have been scheduled by the IT Manager to commence at 23:59 daily on all servers. This allows adequate time for all employees to log off from their workstations and ensure all files located on the servers are closed and ready for backup. Backup includes all data file drives located on the server except the operating system files. 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 "GIAC *Server* FULL *YYMMDD"* (where two digits represent the year, month and date of backup), default media set, verify after backup complete.

Daily Backup Verification

1. From Admin workstation Open ARCserve manager.

2. From the taskbar Manager Click on Job Status.

3. Respond OK to Media Information message from previous nightly backup.

4. Check for "successful" Job Status for the previous night's backup.

5. If the Job Status is anything other than "successful", double-click entry.

© SANS Institute 2000 - 2002 Author retains full rights.

6. Click Activity log File tab and review for errors, if there is no error.

7. Eject current Tape, run cleaning tape for drive

8. If there is error, rerun tape backup with another blank tape, preferably brand new tape if circumstance (time constraints, etc) allows.

9. If time does not allow rerun of the tape backup, the current tape will be marked "BAD-initials" on the tape label so that it can be replaced on an appropriate date during the tape rotation.

10. Close Arcserve manager.

11. Eject tape(s) from tape drive(s).

12. Reload tape(s) based on daily, weekly or monthly tape rotations.

13. Record status as "OK-initials" in the tape backup document for the appropriate date of the previous tape backup.

14. Store the tape(s) in the appropriate tape storage place.

15. Perform same procedure on all GIAC servers making sure to log off of each successive server environment. Policy is given in the IT: Secure Server Environment.

Audit Verification

Since the ITSO is currently unavailable, the IT Manager will temporarily perform the auditing task until the ITSO is appointed. Thus the IT Manager will recover data on a monthly basis in order to perform audits for compliance. Recommendations will be made accordingly to the upper management.

© SANS Institute 2000 - 2002, Author retains full rights.

References

Woods, Charles Cresson, “Information Security Roles and Responsibilities” (Special State of CA Presentation), Department of Information Technology Seminar, 24 April 2001.

Briney, Andy, “Security Focused: Overview, Security Breaches, Risks of E-Commerce, Security Policies”. Information Security Magazine, Vol 3, Number 9. September 2000, pp 40-68.

Erlanger, Leon. “21st Century Security.” Internet World Magazine. December 2001: P.24-25.

Smaha, S. E., Winslow, J. Misuse detection tools. *Computer Security Journal* 10(1994)1, Spring, pages 39-49.

Brenton, Chris, Mastering Network Security, SYBEX, Network Press, 1999.

Kerby, Fred. Defense In Depth. SANS Institute, 2001. Pgs. 3-7.

McKenney, Brian. “Defense in Depth”. The Edge. 5 May 2002.
URL: http://www.mitre.org/pubs/edge/february_01/mckenney.htm

“ASU Computer System Backup Policy”. Arizona Board of Regents. 13 April 2001.
URL: http://www.west.asu.edu/itweb/policies/UnivData/DataBackup.htm

‘‘The SANS Security Policy Project”, SANS Institute resources.
URL: http://www.sans.org/newlook/resources/policies/policies.htm

“Documentation – Cisco 1600 Series Routers”. Cisco Systems.
URL: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1600/index.htm

“Product information on desktop anti-virus corporation edition, and Symantec Security Services”. Symantec Inc.
URL: http://www.symantec.com/product/

“Understanding Internet Information Security”. Microsoft Corporation.
URL: http://www.microsoft.com/ntserver/techresources/security/iissecure.asp

“Detailed View - StandbyServer 5.3 for NetWare”. Novell.
URL: http://www.novell.com/products/clusters/sbs/details.html

Vyncke, Eric. "Pix 515 VPN client using PAT”. Cisco System. 17 July 2001.
URL: http://list.nfr.com/pipermail/firewall-wizards/2001-July/010961.html"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Zamboni, Diego. “Security Policy”. Coast. 20 September 1999.
URL: http://www.cerias.purdue.edu/coast/intrusion-detection/policy.html

VanMeter, Charles “Defense In Depth: A Primer”, February 19, 2001, SANS Information Security Reading Room
URL: www.sans.org/infosecFAQ/start/primer.htm

Landergren, Pia. "Hacker Vigilantes Strike Back." June 20, 2001.
URL: http://www.cnn.com/2001/TECH/internet/06/20/hacker.vigilantes.idg/index.html

“The SANS Security Policy Project”. SANS Institute resources.
URL : www.sans.org/newlook/resources/policies/policies.htm

Information Security Magazine, 20 Dec 2001
URL: http://www.infosecuritymag.com/

© SANS Institute 2000 - 2002, Author retains full rights