Global Information Assurance Certification Paper

GIAC Enterprises

Information Technology Infrastructure, Business Operations & Security Policies

GISO Practical Assignment
Prepared by: **Amer Malik**
GIAC Userid: amalik001
Version: 1.1 - December 2001
Submission: Original (with extension)
Training: Nov 27 – Dec 3, 2001 Conference, Washington, DC

Table of Contents

1 Document Notes

1.1 Definitions

Project = A GIAC Enterprise (business) project is defined as a overall effort for a particular cause that is under a contract by a funding source.

Program = A program is sub-project that addresses a defined task. It is also referred as a subproject.

Country Office = A remote office established in a foreign country of operations.

1.2 Acronyms

Acronym	Description
B-2-B	Business to Business
CDM	Clinical Data Management
CO	Country Office
CRM	Clinical Research Monitor
DMZ	Demilitarized Zone
FDA	Food and Drug Agency
GCP	Good Clinical Practices
IT	Information Technology
LAN	Local Area Network
PC	Personal Computer
SSL	Secure Socket Layer
RDBMS	Relational Database Management System
WAN	Wide Area Network

1.3 General

The text*" [Link]"* refers a location where another GIAC's policy or a document either exists or should exist.

2 GIAC Enterprises (Assignment 1)

2.1 Description

GIAC Enterprises is a non-profit research organization dedicated to improving the quality of life through research, education and promotion of preventive healthcare. It operates in collaboration with a worldwide network of government agencies, research institutions, nongovernmental organizations, and private sector entities. GIAC offers a broad spectrum of technical services ranging from clinical research to advising governments on national health policy.

GIAC Enterprises is structured into two divisions, each of which maintains their own US office. The division offices are in two U.S. locations, North Carolina and Virginia. Each division is functionally independent and has authority and control over its own operations. The North Carolina office is considered to be GIAC headquarters and is home to an executive body that oversees both divisions. GIAC Enterprises has approximately 600+ employees of which 250 are in North Carolina, 150 are in Virginia, and 200 spread among native countries.

The Information Technology (IT) department is an enterprise resource and it serves GIAC's technology needs for all of its offices. Securing information and technology infrastructure is a responsibility and thus a function of IT.

2.2 Business Operations

GIAC Enterprises' business objective is not to increase profitability or market-share; instead, its goals are philanthropic – improve the quality of life, primarily in underdeveloped countries. GIAC Enterprises does not have a sales force and its work product is considered public.

GIAC Enterprises does not have a partnership with any organization that requires another organization to have B-2-B access to GIAC Enterprises' network and computing environment.

As a health care research organization, GIAC Enterprises implements long term (3 – 5 years) projects that involve clinical studies, quality of life surveys and education on preventive health care in the areas of its expertise. It is expected to conform to the practices of good science under the moral and legal obligations and a portion of its work is considered under US Food and Drug Agency's (FDA) regulations.

The following sections briefly describe the organization's major operational areas.

2.2.1 Email & Distribution Lists

Like any other global organization, GIAC Enterprises heavily relies on email systems to conduct its business and manage its work. Under GIAC's business model, each office must be able to conduct its day-to-day operations independently of the head office. This entails that each office

should have an independent email system that replicates user information on a scheduled frequency. Microsoft Exchange is used as the email server at all of GIAC's offices.

GIAC maintains several distribution lists that are associated with projects and affiliated organizations. These distribution lists are maintained via a dedicated Microsoft Exchange server.

2.2.2 Clinical Studies

The clinical trials are conducted to gather and study data about efficacy of health care programs (sub-projects) implemented in various populations around the globe. . From an information security perspective, the compromise of data integrity is the primary risk factor. Only twenty percent of the clinical studies conducted by GIAC Enterprises are submitted to FDA for approval. GIAC Enterprises has implemented processes and procedures that enable the work to be auditable in accordance with FDA guidelines for clinical trials.

All clinical data collected is transferred to the head office data center in NC to be stored, cleansed and analyzed. About 50% of the clinical trials collect data on paper and copies are sent to the head office to be manually entered in a Clinical Data Management (CDM) system that sits on top of Oracle RDBMS. PhaseForward, an industry leading clinical data management software developer, develops the CDM system used at CIAC. Where and when feasible, CDM application's web interface is used for data entry in the field. This data (via the web interface) is entered directly into a database residing on a server at the head office data center. In addition to the access level security the data transmission over the web link is done on SSL and encrypted by the CDM application. The application and the database are housed on a server placed in a DMZ on GIAC's head office network.

During the course of a clinical study, Clinical Research Monitors (CRM) travel to the investigation sites and review project progress and compliance to protocol. While traveling, these CRMs need access to the Internet and GIAC Corporate Network. CRMs are provided with NT/2000 based laptops that have global connectivity service to an ISP via CGINet (service provider). Access to corporate applications is provided over secure ICA connection with Citrix Metaframe. Standard Microsoft Office applications (Word/Excel/Project) are used to track and manage projects.

2.2.3 Quality of Life Surveys

GIAC conducts extensive quality of life surveys to analyze the health care conditions and to determine the success of projects it implements. The survey data is not under the scrutiny of FDA. The data is collected is entered into a PC based data collection application like EpiInfo, Blaze and etc. This data is then transferred into SAS data for further analysis and reporting. The amount of data is under a few megabytes and is easily transferred to the sponsor site (NC or VA) via email or removable media. Analysis and results from survey data are used for publications and designing programs for future.

2.2.4 Finance Operations

Monies are generally awarded to GIAC by funding agencies based on contractual agreements. GIAC then allocates and transfers funds for various projects that come under each agreement.

The two US divisions use the same financial application and databases, which are housed in the data center at the head office. The financal applications run on Oracle and SQLServer databases and are available to the Virginia office over a dedicated T1 WAN link. The finance applications used at GIAC is off the shelf however there are some reporting interfaces built in house.

The Country Offices manage the allocated funds and provide accounting to the head office on monthly basis. The Country Offices log accounting data in a locally deployed application, which is installed on Microsoft NT based workstations. Each quarter a CD accounting data is sent to the head office, where the data is uploaded into the corporate finance database.

2.2.5 Web Access

GIAC employees at all of its offices must have access to The Internet to conduct research, look up project related material and transmit email. The two US office locations are connected to local ISPs via dedicated T1 links. Each Country Office has at least a 56K or better connectivity to its local ISP.

2.2.6 Education and Dissemination of Information

2.2.6.1 Corporate Website

GIAC Enterprises maintains a website that contains most of its research results and relevant information about its work. It is widely and heavily (within its intended audience) used, however, there is no financial or work related transaction that takes place over this website. The website is hosted from the head office data center and the host server is placed in a DMZ.

2.2.6.2 Project Based Websites

GIAC Enterprises manages and hosts project based websites that serve the project community. Like the corporate website, these websites are also hosted from the head office data center and are placed in a DMZ at the Headquarter data center.

2.2.6.3 Publications, Magazines & Presentations

GIAC publishes their research results and other information in a variety of magazines, journals and white papers. This work is a significant source of corporate pride, but does not require any IT consideration from a security perspective since it is public. However, the information within these journals does represent a GAIC business asset, and is mentioned for completeness of the business aspect being discussed.

2.3 IT Infrastructure

2.3.1 Computing Environment

GIAC Enterprises' computer operating environment is mostly Microsoft Windows based with exceptions of a few legacy applications running on Compaq's VMS operating system and some graphics based applications running on Apple's Macintosh operating system. Workstation operating systems is Microsoft Windows 2000 Professional and servers run Microsoft Windows NT or 2000 in a Microsoft Windows NT domain environment. The corporate standard for Intel based servers and workstations is Dell brand.

For virus defense, all Windows NT/2000 based servers run McAfee NetSheild and workstations run McAfee VirusScan. In addition, the MS-Exchange servers run McAfee GroupSheild. McAfee Management Console has been configured to push scan engine and virus pattern files updates to all workstations and each server is configured to pull updates. These updates are scheduled twice per week.

2.3.2 Head Office - Data Center

The head office location in North Carolina serves as the primary data center. Following is a list of important servers and hosts that are housed at this data center:

2.3.2.1 Servers / Hosts

System	Application	Operating System	Network Location
File Servers	Authorized File Access	Dell/ Windows NT	Internal
E-Mail Server	MS-Exchange 5.5	Dell/ Windows NT	Internal
Clinical Servers	Clinical data management	Dell/ Windows NT	Internal
Clinical Server – Web based	Clinical data management	Dell/ Windows NT	DMZ
Legacy Clinical Apps	Clinical data management	Compaq/ OpenVMS	Internal
Finance Servers	Finance Apps & Database	Dell/ Windows NT	Internal
Intranet Server	Intranet	Dell/ Windows NT	DMZ
Intranet DB Server	Database server for Intranet	Dell/ Windows NT	DMZ
Corporate Database Servers	Corporate apps (EIS, Contacts, etc.)	Dell/ Windows NT	Internal
Web Server	Public Web Access	Dell/ Windows NT	DMZ
DNS Server	Systems use	Dell/Windows 2000	Internal
Wins Server	Systems use	Dell/ Windows NT	Internal
Print Server	Systems use	Dell/Windows 2000	Internal
DHCP Server	Systems use	Dell/Windows 2000	Internal
Citrix Server	Remote connectivity	Dell/Windows 2000	Internal
Shiva	Remote dial in	Shiva.Shiva OS	Internal

2.3.2.2 Networking Equipment

System	Model/Vendor	Model
Edge router	Cisco	3640
Firewall (External)	Cisco	Pix-515
Firewall (Internal)	Cisco	Pix-515
Core Router	Cisco	3661
Core Switch	Cisco	CAT 6509
Switches	Cisco	Catalyst-4006, CAT 2824
VPN	Cisco	3015 – VPN concentrator

2.3.2.3 DMZ

Demilitarized Zone (DMZ) in the Network topology diagram in this document is conceptualized with a single box, however the actual implementation is a multi-zone solution. DMZ is established by implementing two-firewall solution. The addressable DMZ interfaces on the external firewall are utilized to setup multiple DMZs. DMZ 1 contains Internet website, DMZ 2 contains Intranet and supporting database servers, DMZ 3 contains VPN, and other system management servers (syslog, etc.) and DMZ 4 contains clinical applications web interface.

2.3.3 Arlington, VA Office

2.3.3.1 Servers / Hosts

System	Application	Operating System	Location
File Servers	Authorized File Access	Dell/ Windows NT	Internal
E-Mail Server	MS-Exchange 5.5	Dell/ Windows NT	Internal
Citrix Server	Remote connectivity	Dell/Windows 2000	Internal
Database Server	Local apps	Dell/ Windows NT	Internal

2.3.3.2 Networking Equipment

System	Model/Vendor	Model
Edge router	Cisco	2601
Firewall	Cisco	Pix-515
Core Router	Cisco	3661
Switches	Cisco	CAT 2924

2.3.4 Country Offices

2.3.4.1 Servers / Hosts

System	Application	Operating System	Location
File Servers	Authorized File Access	Dell/ Windows NT	Internal
E-Mail Server	MS-Exchange 5.5	Dell/ Windows NT	Internal

2.3.4.2 Networking Equipment

System	Model/Vendor	Model
Firewall	Cisco	PIX-501

2.3.5 Internet Connectivity

In the US, each of the two offices is connected to an ISP and to each other via a dedicated T1 link. Country Offices have a 56K or better connection to a local ISP.

2.3.6 Remote Connectivity

1. Each traveling user's laptop is equipped with GGINET software & service that allows for an Internet connection through a local ISP worldwide.

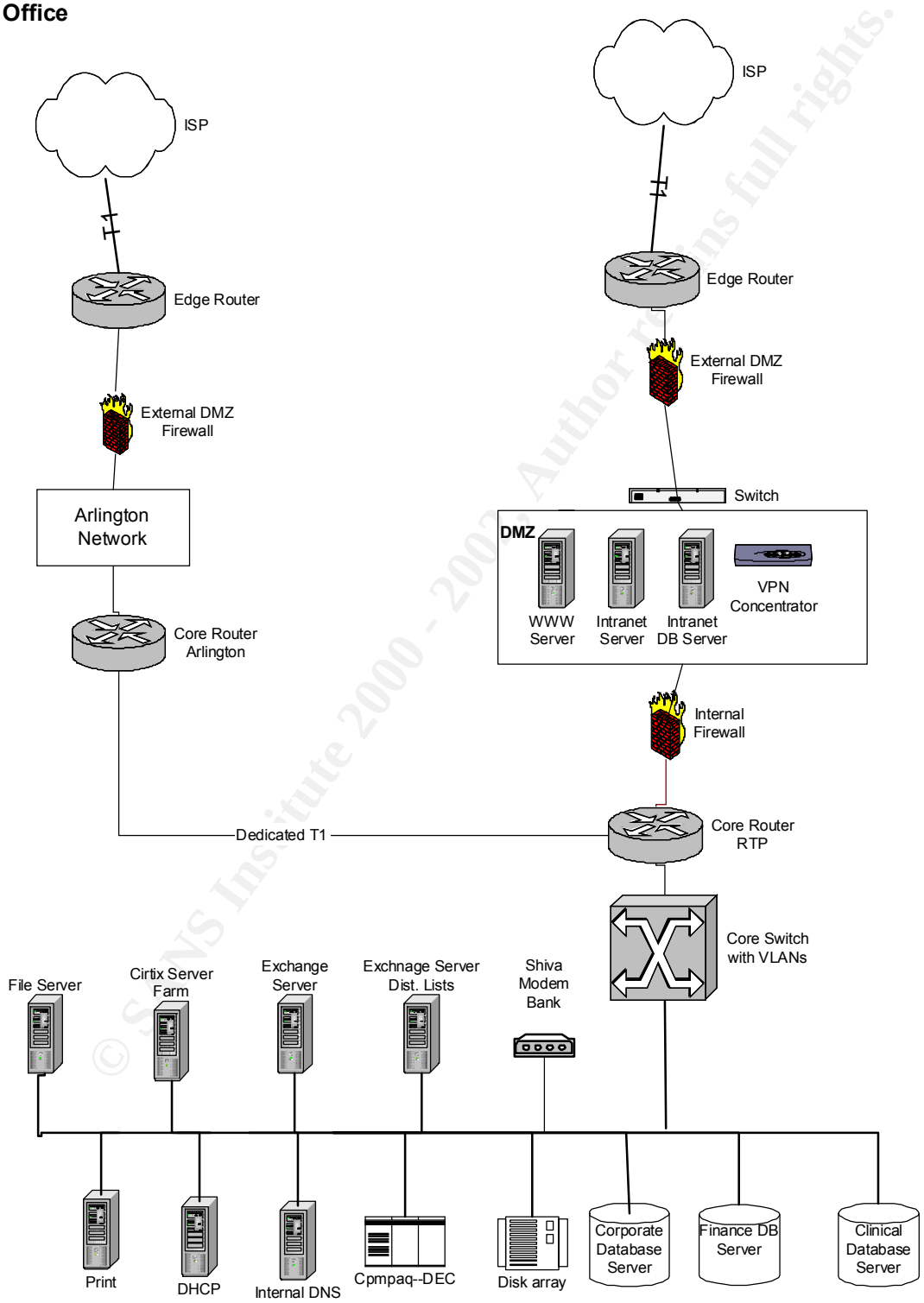
2. Citrix Metaframe is used to provide secure ICA access into GIAC's NC and VA offices. This access is established over the Internet connectivity. The Citrix server farm is located in a VLAN with restricted access to rest of GIAC's network.

3. VPN connectivity is provided via a CISCO concentrator that is deployed in the DMZ. Currently the access through VPN is limited a select group with restricted functionality.

4. A Shiva server that manages a bank of modems supports direct dial in via toll free numbers. The Shiva solution is being phased out and only a few employees have access to GIAC's network through it. There is limited access to remainder of the network from the VLAN Shiva is placed in.

2.4 Network Topology

GIAC Network Topology :
Head Office



3 Security Policy (Assignment 2)

3.1 Areas of Risk

"The best choice for a security implementation is the one that best fits the business context and will be used" (Joyce Graff, Gartner, Securing the Infocosm, June 2001, Orlando, Florida).

Using ***Risk = Value x Threat x Vulnerability*** as the guiding formula, an assessment of current information security risks was conducted. Executive Management, Operational Staff and Technical Staff were interviewed and assisted in the development of a realistic and practical discussion of information security and related issues as they pertain to GIAC Enterprises.

Several principles were adopted as guidelines in the determination of information security risks:

- GIAC must be a good cyber citizen by securing its computing environment.
- GIAC places a high value on its reputation and integrity of its work.
- GIAC's computing environment does not impact its revenue prospects.
- No financial transactions are conducted over any website managed by GIAC Enterprise.

The following areas are of particular concern to GIAC Enterprise:

1. Virus Infections
2. Infrastructure Security
3. Data and Application Security
4. Social Engineering
5. Misuse of corporate information technology (IT) systems

3.1.1 Virus Infections

3.1.1.1 Threat

Virus is any code, script or software that compromises computer systems causing unintended prejudicial actions. System vulnerabilities are exposed with each upgrade and addition of new software, which is an unavoidable fact of current computing environment. Viruses are becoming more sophisticated with time and virus developers are increasing. Considering the computer virus related headlines during past year, predictions from Gartner and exploitations reported on SANS, CERT and other such organizations the threat is unquestionably significant for any corporation that relies on its computing environment to conduct day-to-day operations.

3.1.1.2 Relevance to GIAC

Due to the nature of GIAC's work it is difficult (if not impossible) to quantify financial loss by a unit of system downtime. A compromised system or systems could result in loss of services and therefore loss of productivity, which depending on criticality of services and data loss could be significant. Another damaging consequence of infected systems is that they could possibly spread the viruses to other organizations that GIAC has business dealing with. This could damage GIAC's reputation for its ability to protect and contain its computing environment. This

is especially pertinent to GIAC's email systems, which are the means of communication with funding organizations. It is only a slight mental jump to equate a compromised computing environment with a compromised project effort.

3.1.1.3 Vulnerability

At GIAC, as in most other US corporations, there is heavy email traffic from outside the corporation which is a major risk area for virus intrusions. Employees also have unlimited access to the Internet at work, from which they could easily download a corrupted file. Infected files could also be introduced to the system via floppy disks, cdroms, or other external media. Furthermore, employees connect to GIAC's network either via a dial-in modem or over the Internet to a Citrix server farm. The computers that are used to establish these remote sessions could be infected and thus could possibly infect GIAC's systems.

3.1.1.4 Mitigation

First and foremost point about the anti-virus mitigating plan is that it must be routinely evaluated and updated as this particular threat is constantly changing. There are several mitigating steps that should be implemented:

- Establish an Anti-Virus Response Team that is responsible for implementing protective measures.
- Define and implement an Anti-Virus policy.
- Deploy Anti-Virus software on all servers and workstations, with automatic updates.
- Deploy Anti-Virus shield on email servers that scans all incoming and outgoing emails.
- Deploy Anti-Virus software at the perimeter of the network to disinfect mail accessed on non-GIAC email servers.
- Select Anti-Virus products from different vendors; for example, use one vendor for servers and workstations and another for perimeter.
- Keep up the upgrades for servers – Define "server hardening" standards and enforce with routine verifications.
- Establish a periodic schedule to research current and new virus alerts.

4 Infrastructure Security

4.1.1.1 Threat

This threat covers a broad category that consists of network, servers, workstations and other network-attached devices. Although GIAC does not have a market position that makes it a likely target for attackers, the unpredictable nature of attackers and the potential loss of operational capability makes an infrastructure breach a high threat to all technology dependant corporations.

It is important to understand the potential security breaches with all of infrastructure pieces in perspective. Infrastructure environment is ever changing with frequent software, hardware and firmware upgrades and additions, exposing new vulnerabilities. These vulnerabilities are being exploited by an increasing number of hackers with or without an agenda against GIAC Enterprise's interests. The attacks could be initiated either externally or internally. A disgruntle or mischievous employee could gain access by running password cracking tools or "sniff" the

network. Such an employee could instill a variety of malicious programs on behalf of other employees and obscure his/her identity.

Some of the attacks in this category are Denial of Service, Distributed Denial of Service, Session Hijacking, SYN Flooding, Ping of Death and other attacks that exploit networking protocols, operating system and the Internet browser vulnerabilities.

4.1.1.2 Relevance to GIAC

Depending on the level of damage, GIAC could potentially suffer a loss of one or multiple services for a length of time that could hinder the work in progress. Likelihood of a far-reaching damage is minute, since at GIAC there is NOT a significant inter-dependency of applications and information. Moreover, a reliable backup and recovery procedure minimizes the length of recovery, thus limiting the damage.

Another aspect of damage to GIAC, similar to viral infection, is reputation loss. Especially when GIAC infrastructure is compromised and unknowingly aid in attacks on its cooperating organizations and business affiliates. Examples of such an attack are spamming, DDoS and other attacks that utilize computing power of an organization.

Recovery from infrastructure compromises could consume significant resources as the detection of problems in this category are complex. Not only must the recovery operation be carried out, but also a thorough system cleansing the must be done. Both operations can be quite time consuming. Another consequence of damaging infrastructure breaches is that it could result in loss of confidence in IT's competence regardless of circumstances.

4.1.1.3 Vulnerability

GAIC's greatest vulnerability is this category is IT staff experience and the lack of an official infrastructure security team. There is increasing demand for extranet (employees use only) and number of project related websites, thus increasing incoming transmissions. With over 40 servers in North Carolina (head office) and Virginia offices and 20+ units of various networking and connectivity equipment with application specific requirements for patches and upgrades, the entire environment as a whole is quite permeable. Compounding the problem is that exploits are being discovered at a rapid pace with unpredictable pattern of attacks and attackers.

4.1.1.4 Mitigation

Securing the technology infrastructure is a tedious ongoing task that requires dedicated resources not only to monitor and manage but also continuously learn new techniques to protect the infrastructure. Securing the infrastructure can only be achieved though a comprehensive plan that enforces rigorous procedures for monitoring and verification.

- Create an infrastructure security team and facilitate ongoing training.
- Create and maintain an inventory of all access points into the network.
- Define and implement networking connectivity security policy.
- Define and implement a server hardening (including security) procedure.
- Implement Least Access Principle for access control.

- Contract with a security vendor to provide routine infrastructure security analysis. Gartner has projected that by 2005 most organizations will rely on specialized vendors to provide adequate security needs.
- Implement a host base and/or a network intrusion detection system.

4.1.2 Data and Application Security

4.1.2.1 Threat

Research by the Gartner Group indicates that over 90% of data theft takes place while data is at rest. Meaning that data is compromised not in transaction but from the database itself. Particular data could have a value that attracts an individual or an interest group to exploit the vulnerabilities of corporate computer systems and steal, destroy or manipulate information. For most corporations the data is the real asset stored either in databases or directory structures. Often applications that provide an interface to data have weak authentication mechanisms. Even if a database has strong authentication and rule based access levels, an application (popular ASP code for example) could provide a tunnel into a database. Generally there are several maintenance or job scripts stored on database servers that do various routine tasks for Database Administrators. These scripts have privileged username and passwords embedded into them and can be easily compromised if file level access in not restricted properly.

4.1.2.2 Relevance to GIAC

GIAC Enterprises has industry recognition for its leadership, integrity and quality of its work product. Data integrity is of a high value to GIAC's mission and its continued success. Moreover, a portion of its work (clinical studies) must comply with FDA guidelines and Pharmaceutical industry's recognized Good Clinical Practices guidelines. Both of mentioned guiding principles require GIAC to regulate its data capturing, managing and reporting procedures and practices. Failure in maintaining the integrity of its data could result in penalties from FDA, loss of contracts and most of all loss of reputation in scientific and research community. In summary, this particular category is of very high importance to GIAC.

4.1.2.3 Vulnerability

The author's view based on experience at GIAC and previous employers that database security is NOT well understood and often a secondary aspect of information security. The applications and the underlying databases are simply web-enabled and are exposed to the Internet without relevant security measures in place. Programmers generally lack an understanding of the available security aspects, and software project security is usually minimal at the best.

There are numerous vulnerabilities in this category; poor access control, lack of security awareness among users, lack of security functions in applications and substandard security procedures at database level. One or more of these weaknesses make the data vulnerable and could lead to successful hacking resulting in corrupt or manipulated data.

4.1.2.4 Mitigation

The following actions should be taken to mitigate data integrity violation:

- Implement reliable backup and recovery procedures with routine testing.
- Raise user awareness regarding information security.
- Enforce strict access controls and integrity rules of databases
- Integrate security features in in-house developed applications at design stage.
- Implement aggressive database access authorization procedures.
- Enforce access to data in databases via store procedures.
- Pay special attention to security for applications and databases being exposed to the Internet.

4.1.3 Social Engineering

4.1.3.1 Threat

"Social engineering remains the single greatest threat to enterprises."(Rich Mogul, Gartner, Securing the Infocosm, A3, June 2001). Successful social engineering could partially or completely circumvent an organization's security system. The hacker gathers information to establish trust, which is then exploited to achieve his/her objective. Most employees are not aware of the always-evolving and creative methods of social engineering and does not give due care to the protection of passwords. A really strong password is of little consequence if not protected properly. Former disgruntled employees and special interest groups are another likely threat that could possibly materialize. Some of the common deception practices are identity theft, playing the partner, acting as an IT authority, playing the support and maintenance role (non-IT) and reverse social engineering (where a target contacts the attacker) and many permutations of the listed and unlisted possibilities. In all of these exploits the target is coerced into revealing information.

The book, Cyberpunk, Outlaws and Hackers on the Computer Frontier by Katie Hafner and John Markoff, states that Kevin Mitnick, the infamous hacker, acquired 80% of the information about a network from social engineering techniques. Recognizing the inherent vulnerable human nature, social engineering should be considered as real of a threat to information security as anything else out there.

4.1.3.2 Relevance to GIAC

The consequences of compromised systems and information at GIAC due to social engineering are the same as mentioned in all of the other risk area described in this document, therefore not repeated in this section.

4.1.3.3 Vulnerability

Essentially anything that stores, shares and represents information about an organization is a point of vulnerability. Social engineering attacks are as numerous and diverse as people performing them. Social engineers can use information produced by an employee of a group within an organization to gain trust elsewhere in the organization. For example, learning about a system's particulars (IP address or name or an application) allows an attacker to present himself/herself as a privileged user like an IT administrator or technician. An attacker can use any scrap of public or private, sensitive or insensitive information. GIAC is quite vulnerable to social engineering because of the general perception of employees about the organization's non-

profit status and non-competitive academic work environment, which leads to a relaxed attitude about information security.

4.1.3.4 Mitigation

- Develop and maintain a social engineering awareness program with mandatory participation.
- Develop a policy that deals specifically with social engineering issues.
- Provide prominent and frequent notifications about password protection guidelines.

4.1.4 Misuse Of Corporate IT Systems

It is the responsibility of a corporation to know how its computing resources are being utilized. The US courts have been holding corporations accountable for actions of their employees when using corporate computing environment. This section will describe three risk areas that stem from non-work related use of computing resources at GIAC.

4.1.4.1 Threat

1. Inappropriate use of email or the Internet that is offensive in sexual, racist or a variety of defamatory contexts can be a liability to the corporation if taken to the US courts.
2. Infringement of copyright laws resulting from unapproved downloads from the Internet or distribution of copyrighted electronic material such as publications, software, games, screen savers and etc.
3. Loss of productivity and ISP-connection bandwidth strain due to excessive non-work related use of the Internet.

4.1.4.2 Relevance to GIAC

GIAC Enterprise receives funding from the US government agencies and many other private philanthropic foundations. The majority of funds are supplied by the US government, which has strict standards for its contractors' work environment. GIAC prides itself on its philanthropic work in advancing health for underprivileged women and children and it would be detrimental to its image if it has to fight court cases of discrimination, harassment, and offensive nature especially against issues dealing with exploitation of women and children. The ramifications from infringement of copyright laws could result in system audits and monetary penalties. At GIAC, productivity loss due to non-work related use of computing environment is difficult to measure, however, it is reasonable to assume that many Internet related activities (eBay, shopping, gambling, games, etc.) are time consuming and would result in significant amount of lost time.

4.1.4.3 Vulnerability

GIAC's is a very diverse and multi-cultural organization employing over 600 people with various standards of forbearance. It's work and work style leads to a work environment that is relaxed and tolerant. A considerable risk exists where one or more employees offend or harm another person or a group of people inside or outside the organization resulting in a corporate liability.

4.1.4.4 Mitigation

- Define and implement an acceptable use policy.
- Educate users about consequences of inappropriate use of corporate computing resources.
- Deploy Web traffic monitoring tools, such as WebSense.
- Deploy a PC auditing tool to track unauthorized and unlicensed software, such as ExpresMeter.
- Implement operating system authorization policies to restrict users ability to modify system configurations and install software.

4.2 Security Policy

In case of an automobile, the purpose of brakes is to enable an automobile to "go fast" and the function of brakes is to "stop" an automobile. Similarly, in case of information security plans, the purpose of security is to enable an organization to conduct its business freely and the function of the security is to secure the computing environment on which a business relies upon. Properly designed and implemented security policies and procedures not only protect information and people but also provide a balance between functionality and access.

Based on the information security training, experience and knowledge gained from extensive discussions within GIAC and the industry experts, it is author's strong opinion that the information security policies be precise, unambiguous and enforceable. "*Like a good marketing campaign, the security campaign needs to be rolled out, accompanied by well-crafted material and training programs." Mary Pat McCarthy & Stuart Campbell, Security Transformation, p69.* In order for security policies to succeed, executive management must endorse and enforce these policies with full support on investment in necessary training.

For GIAC, it is recommended that an Information Security Committee (ISC) be created with representation from Executive Management, Operational Management, Information Technology and Human Resources. This ISC would be responsible for overseeing security plans implementation and routine audits. All information security policies must be reviewed, updated (if needed) and signed off on annual basis. This requirement should be considered as a part of the policies described below:

4.2.1 Acceptable Use Policy

Development of this policy leveraged on portions of 'Acceptable Use Policy' on SANS Institute Resources website as well as Yale university's Appropriate Use Policy (See References). Some of the language is derived from the two mentioned sources.

4.2.1.1 Purpose

- To mitigate risks associated with misuse of GIAC's computing resources.
- To ensure that GIAC's computer resources are used for their intended purpose.
- To define the rules for appropriate use of GIAC's computing resources.

4.2.1.2 Scope

This policy applies to anyone using GIAC Enterprise's computer resources. Here 'computer resources' include all corporate owned or leased server, workstations, Laptops, PDAs, mobile phones, Internet/Intranet/Extranet access, network infrastructure, and any other device/system that is attached to GIAC's technology infrastructure.

4.2.1.3 Policy Statements

4.2.1.3.1 Fundamentals

1. GIAC reserves the right to audit and monitor its computing environment on a periodic basis to ensure compliance with this policy.
2. Computer resources should not be used for non-business reasons in ways that interfere with any employee's performance of normal duties.
3. Some approved employees may be exempted from certain restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
4. When the 'reasonableness' or legitimacy of use of a computer resource is uncertain, the issue must be escalated and resolved by a supervisor.
5. Any use of computer resources that is not described in this section should not be considered acceptable by default.

4.2.1.3.2 Systems and Information Security

1. Employees have a responsibility to take all necessary steps to prevent unauthorized access to corporate information they are exposed to.
2. All login screens should display a notice about prohibition of unauthorized use.
3. System level passwords should be changed every two months.
4. User level passwords should be changed quarterly
5. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
6. Use encryption of information in compliance with GIAC's Acceptable Encryption Use policy [Link].
7. Laptops should be protected in accordance with the "Laptop Security Tips" [Link].
8. A disclaimer stating that the non-business related content in the email does not represent GIAC's position should be attached to all GAIC originated emails.

4.2.1.3.3 Unacceptable Use

The following activities are strictly prohibited, with no exceptions:

In Violation of Laws

1. Under no circumstances is an employee of GIAC Enterprise authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing GIAC owned resources. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by GIAC.
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which GIAC or the end user does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

System and Network Activities

1. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
2. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
3. Making fraudulent offers of products, items, or services originating from any GIAC account.
4. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
5. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
6. Port scanning or security scanning is expressly prohibited unless prior notification to Information Security Committee is made.
7. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
8. Circumventing user authentication or security of any host, network or account.
9. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
11. Providing information about, or lists of, GIAC employees to parties outside GIAC.

Email and Electronic Communications

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or content of messages.
3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within GIAC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by GIAC or connected via GIAC's network.

4.2.1.4 Responsibility

- The Information Security Committee (ISC) will be responsible for creating guidelines concerning personal use of the Internet/Intranet/Extranet and all other computer systems.
- ISC is responsible for maintaining this policy
- ISC with Executive Management's support and approval is responsible for enforcement of this policy.
- ISC is responsible for performing audits and reporting to Executive Management annually.

4.2.1.5 Action

1. New employee orientation must include this policy and related training material.
2. The review of this policy and completion of associated training material [Link] should be a part of employees' annual performance appraisal process.
3. This policy may be updated and enforced prior to its expiration to ensure security of corporate interests.

4.2.1.6 Compliance

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

4.2.2 Social Engineering Awareness Training Policy

4.2.2.1 Purpose

- To mitigate the security risks associated with lack of social engineering awareness.
- To incorporate social engineering defenses into security plans.

4.2.2.2 Background

If social engineering defenses are not incorporated into overall security plans, then all other defensive measures could potentially be invalidated. For a comprehensive and realistic security plan, social engineering awareness must be a part of security awareness efforts. GIAC recognizes that properly trained people are its best defense against social engineering and vise versa biggest vulnerability if not educated.

4.2.2.3 Scope

This policy applies to anyone using GIAC Enterprise's computer resources. The term 'computer resources' include all corporate owned or leased server, workstations, Laptops, PDAs, mobile phones, Internet/Intranet access, network infrastructure, and any other device/system that is attached to GIAC's technology infrastructure.

4.2.2.4 Policy Statements

- Defense against social engineering must be a part of GIAC's overall information security plan.
- Ongoing education on social engineering must be facilitated for all levels of organization.
- GIAC employees should be aware of their responsibilities in protection against social engineering exploits.

4.2.2.5 Responsibility

Information Security Committee is responsible for development and implementation of this policy.

4.2.2.6 Action

1. Deploy a web-based training program on the corporate Intranet.
2. Require GIAC employees to complete the training program once every year.
3. Enforce strict password policies.
4. Train users to develop relatively secure, yet easily memorize-able passwords.
5. Assist departments in development of a list of "holes to cover" based on user-access levels. For example, the Information Technology department must have a comprehensive list of access points into GIAC's computing environment for a systems analyst. Upon departure of a systems analyst, changing passwords will ensure security for all identified access points.

4.2.2.7 Compliance

- Review of this policy should be a mandatory requirement for each employee's yearly professional development plan.

- Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

4.2.3 Anti-Virus Infection Policy

4.2.3.1 Purpose

- To define rules and requirements for GIAC computers for prevention of viral infections.
- To mitigate risks from viral infection of GIAC computers.

4.2.3.2 Scope

This policy applies to all computers owned or leased by GIAC Enterprise. Here computers include servers, workstations and laptops.

4.2.3.3 Policy Statements

General

1. IT must maintain an anti-virus response team and response procedures.
2. A general guideline should be posted and kept up to date on the corporate Intranet.

Workstations

1. Anti-virus software must be configured to run at boot time on all workstation.
2. Anti-virus software application engines and virus-prevention updates must be pushed to the workstations.
3. Workstation users are prohibited from disabling the anti-virus application for any reason.

Servers

1. All Windows NT/2000 production servers must be configured run an anti-virus application upon startup.
2. Anti-virus software must be configured to receive application engines and virus-prevention updates automatically.
3. System administrators are prohibited from disabling the anti-virus application on any server, unless approved by IT department head or ISC.

Note: For Compaq/OopenVMS system there are no known virus infection vulnerabilities, therefore, no anti-virus is recommended for this system.

Email Systems

1. A virus-scanning solution must be implemented at the network perimeter to scan and either disinfect or remove all incoming and outgoing email.
2. Anti-Virus software must be configured to monitor and cleanse email server
3. The Anti-Virus software on email server and the virus scanning software deployed on the perimeter should be from different vendors.

4.2.3.4 Responsibility

- Anti-virus response team is accountable for implementation and administration of the requirements defined in this policy.

- Information Technology department head is responsible for enforcement of this policy.

4.2.3.5 Action

- The infected system should be immediately shutdown if a vaccine is not available.
- All virus infection reports from users must be verified.
- When a real outbreak of a virus is verified, Anti-Virus Response team must notify all corporate offices with mitigating steps.

4.2.3.6 Compliance

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5 Security Procedures (Assignment 3)

5.1 Anti-Virus Operational Qualification Procedure

This section will define procedural requirements for server and workstation only. The perimeter anti-virus application is deployed on a single server and should be under a contract with a reseller for upgrades and monitoring.

5.1.1 Servers

5.1.1.1 Responsibility

Due to the severe consequences of virus infection of a server [section 3.1.1.2] it is critical that the anti-virus applications are installed and configured properly for optimal operation. At GIAC servers are responsibility of Systems Analysts team; therefore, a member of System Analysts group must perform the steps described below.

5.1.1.2 Configuration Procedure

1. Install the anti-virus application from the secure network location [location link] onto a new or rebuilt Windows NT/2000 server that is connected to the GIAC network.
2. Reboot server to verify a clean startup.
3. Verify if the anti-virus application is running as expected.
4. Install a version of virus pattern file and a scan engine that are prior to the most recent version.
5. Schedule the anti-virus application to get updated virus pattern files and engine updates from the vendor web site within a few minutes.
6. Configure the application to send emails to Anti-Virus Management team when new patterns file and scan engine updates have been received.
7. Verify the update in the application log once the scheduled time has passed.
8. Verify the receipt of email notification.
9. If any of the features configured are not working, troubleshoot problem until resolved.
10. Schedule the updates for 4:00pm daily.
11. Verify the update attempts the next day.
12. If the anti-virus application is working as configured, release the server for intended use.
13. Install other software/applications on the server as needed.
14. Reboot server to verify a clean startup.
15. Verify if the application is running normally.
16. Note the date and time of these activities in the server log [Link to the document location]

5.1.1.3 Verifications

- On a weekly basis, the scheduled Systems Analyst must report to his/her supervisor regarding the operational status of anti-virus application on all production servers.

- All System Analysts should be setup to receive notification regarding new updates from anti-virus vendors.

5.1.2 Workstations

5.1.2.1 Responsibility

At GIAC workstations are configured and managed by the Help Desk group. A management console is configured to "push" the updates each time a workstation starts up and two other times per week if it remains logged on to the network during the week. Once a workstation is added to the GIAC network, it is automatically added to the console's master list. However, for organizational purpose, the console administrator manually assigns the newly added workstations to logical groups.

5.1.2.2 Configuration Procedure

1. Install the anti-virus application from the secure network location [location link] onto a clean Windows 2000 workstation that is connected to the GIAC network.
2. Reboot workstation to verify a clean startup.
3. Verify if the anti-virus application is running as expected.
4. Configure anti-virus application to obtain updates from the anti-virus server each time the workstation reboots and every Tuesday and Thursday.
5. Install other GIAC standards applications
6. Verify if anti-virus application is running as expected.
7. Resolve any application related issue if present.
8. Generate a manual "push" from the anti-virus management console.
9. Verify the update at the anti-virus management console.
10. Release the workstation to be supplied to the user.

5.1.2.3 Verifications

On a weekly basis, the scheduled Help Desk member must report to his/her supervisor regarding the anti-virus application update status of workstations attached to GIAC network.

6 References

1. Information Security Conference: Securing the Infocosm, a Gartner Conference, June 11-13, 2001, Orlando, Florida

2. SANS Security Project http://www.sans.org/newlook/resources/policies/policies.htm

3. Cyberpunk, Outlaws and Hackers on the Computer Frontier by Katie Hafner and John Markoff

4. Security Transformation by Mary Pat McCarthy & Stuart Campbell

5. http://www.yale.edu/policy/itaup.html for Appropriate Use Policy

6. http://www.CERT.org

7. This document took many clues for style and development of language from several previous GISO and GISW assignments posted on GIAC's website, however no particular assignment was cited within the sections above due to lack of direct reference to the material and similarity of my direction with portions of material read. Nonetheless, in appreciation of other students' efforts, mentionable assignments are Ray_Slepian_GISO, John_Ford_GISO, John_Pistilli_GISO and Asad_Alsadar_GISW.