Global Information Assurance Certification Paper

Information Security Officer Training

GISO Basic Practical Assignment

Version 1.0 (October 31, 2001)

SANS Network Security, San Diego, CA
October 15 - 22, 2001

Randy Patterson

Submitted December 2001

Table of Contents

Assignment 1: Describe GIAC Enterprises

Describe GIAC Enterprises (20 points) This section is intended to provide a brief description of GIAC Enterprises, its information technology (IT) infrastructure, and its business operations. Understanding these elements is key to defining an appropriate security policy.

1.1 Assigned Task

Description of GIAC Enterprises

- Include a brief description of GIAC Enterprises and the nature of its business (hospital; e-commerce site; non-profit organization; manufacturing; etc.).

IT Infrastructure

- Include a description of the IT infrastructure of GIAC Enterprises – the network(s) and resources that you are trying to protect. You should include:
    - A diagram of GIAC Enterprises' network. You may include an actual diagram or a conceptual diagram. However, your diagram should include enough detail to distinguish among private (internal) networks, public networks, and the Internet. It should also include the location of key components (i.e., important servers, routers, firewalls, intrusion detection systems) that are relevant to GIAC Enterprises' infrastructure.

- Your network must include at least the following components:
    - a router;
    - a firewall;
    - an internal (private) network;
    - a screened subnet or demilitarized zone (DMZ) for public servers (web, mail, DNS, etc.);
    - a VPN or other secure remote access (for business partners, remote users, etc. as appropriate);
    - any key servers relating to GIAC's particular business (file servers, database servers, etc.).

Be sure to list relevant information about the components (hardware brands/versions; operating system type/version; etc.) and their configuration (services/applications running; etc).

Business Operations

- Briefly describe the operational IT needs for GIAC Enterprises and its employees. How does GIAC conduct its business? Do customers, business partners, or suppliers need to connect to the network to send or receive information? How is this done? What types of applications and access do employees need? Are there any remote users (salespeople, telecommuters, employees on travel, branch offices) that require access to the network? How is this done?

- This section effectively defines the applications, services, and types of access (inbound and outbound) that are necessary for GIAC Enterprises to operate. This information is essential for defining your security policy below.

1.2 Description of GIAC Enterprises[1]

GIAC Hospital Enterprises, the state's largest, not-for-profit medical center, has served the region since 1925, consistently offering a wide range of programs and services to meet virtually all medical needs. GIAC provides a combination of professional expertise, state-of-the-art technology, old-fashioned care and compassion.

In the last decade alone GIAC Hospital has invested more than $165 million in the construction of new facilities and introduced some of the most innovative services and programs in the healthcare industry.

Through the years they have grown to become the state's largest hospital. Licensed for 705 patients with 54 skilled beds, GIAC's main campus covers nearly two million square feet and spans more than six city blocks. They have built an unprecedented network of facilities that make GIAC's quality care easily accessible from almost every neighborhood in our city and region.

1.3 IT Infrastructure

GIAC Enterprise's divides it's network structure into internal, external and DMZ segments (figure 1.3.1).

[1] Section 1.2 Modeled from http://www.[edited name].com/about/about.html

1.3.1. GIAC Enterprise Network Diagram

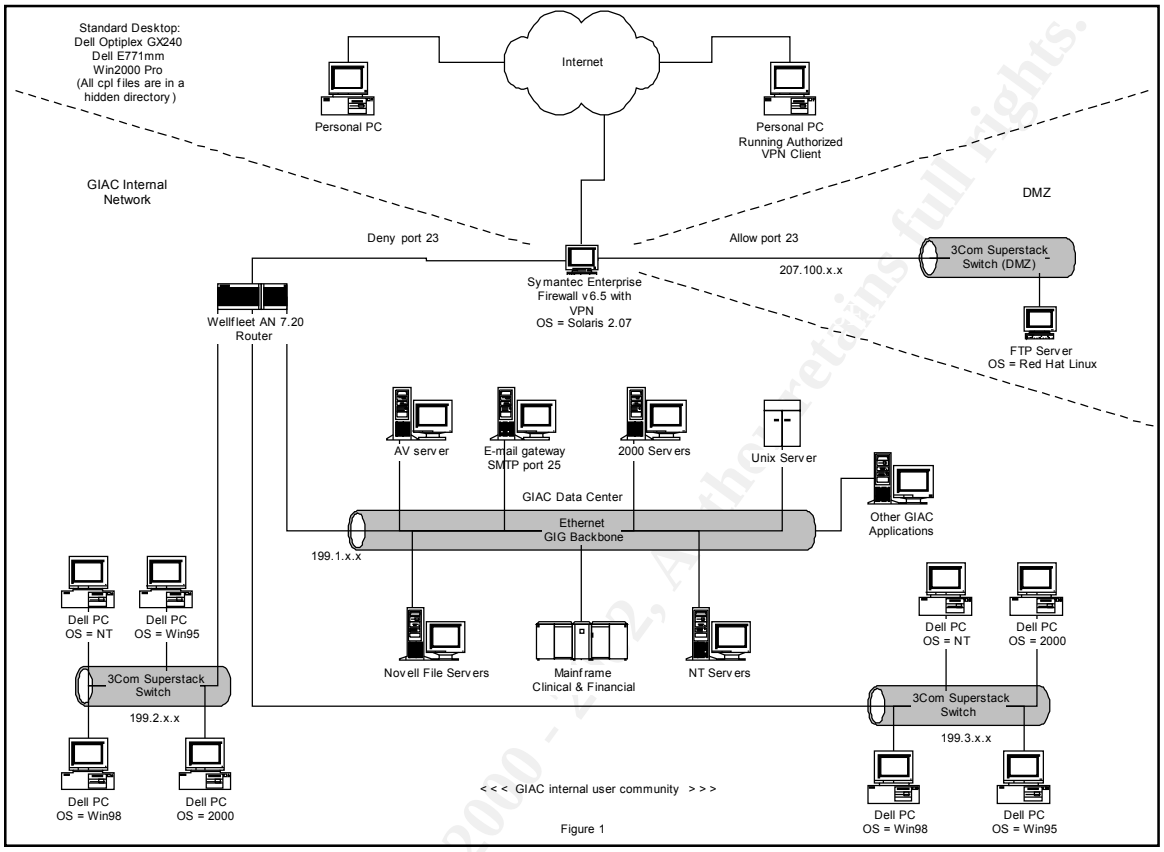

Figure 1

GIAC Enterprise's internal network includes clinical, financial, laboratory systems as well as email and office automation applications. To each of these systems are connected various server based applications for specialized departmental use. The clinical information system and financial applications all run from an IBM mainframe computer. This system is integrated with an Interface engine running on a RISC6000 which connects with the billing system running on an IBM SP2 based RISC6000 server. The surgery system is also interfaced to the billing system.

The internal networking is mostly LAN connections using IP addressing. Wiring is a combination of fiber and category 5 wiring with some limited category 7 wiring. The desktop computers distributed on a floor are all tied back to wiring closets. The closets are redundantly connected and tied back to concentrators on each floor. The floors at then redundantly connected within the buildings. All connections eventually tie back to a WellFleet Gigabyte backbone in the data center.

Local access to the various applications is allowed only after a network connection is established. A network administrator manages all wall jacks and connections are allowed only when sufficient documentation is submitted and security standards for a

desktop PC have been met. Portals through the firewall are managed by a firewall administrator and allowed only when sufficient documentation is submitted and security standards for firewall modifications have been met.

The IT Department reports to the CIO who reports to the CEO. IT is managed by functional groups and divided into Applications and Customer Services & Technology. IT is not an application development shop but rather chooses to install best of breed applications tied together by interfaces. IT provides limited development of customized functions and utility applications. The IT Application Area provides support for all clinical and financial systems. The IT Infrastructure Area provides support for the technological areas and data center operations. This includes Telecom / Servers & Networks, Data Center Operations, PC Desktop Support and Help Desk / Inventory.

The IT Server Group includes the system administrators. This group is comprised of operating system administrators, network administrator, firewall administrator, web administrator and anti-virus administrator. This area, along with the IT Security Manager and PC Desktop Support, is primarily responsible for design, implementation and support of IT security initiatives.

1.4 Business Operations

GIAC Enterprises provides electronic connectivity from all it's campus buildings back to the main data center located in the central campus building. All main computer equipment, servers, production printers and telecom equipment is housed within the data center and users are connected via redundant fiber paths. The data center is a 24x7 secured area and has physical access controls using a system of magnetic key locks with an integrated camera system for all access points and monitored round-the-clock by a security department. Employees may enter and exit secured areas of the facility using swipe badge readers.

The hospital has an integrated information delivery system that connects several mainframe, mid-range and server based systems. These host applications support all critical hospital operations. The data center has redundant and alternate utility sources (electricity, phone service) as well as an integrated UPS and backup power generator system that allows the hospital to completely function without outside support. By law the electrical system is tested monthly and must be able to sustain uninterrupted services for several hours.

All system access is controlled by individual user id and passwords. Users must authenticate to the network servers (Novell) before being granted access to any GIAC application. Applications for user ids must be completed prior to being issued for each of the departmental systems. Passwords must conform to policy specifications which dictates length, syntax, change frequency and invalid entry lockout parameters.

Users are provided PC equipment that have been imaged and configured to a corporate standard. User modifications to system configurations are not allowed and controlled by

locking down the control panel. A standard imaged system will provide for the common components to the desktop, prevent user access to the control panel, establish the anti-virus protocol, housewide applications, connection to the email system, automated screen saver activation, etc.

GIAC Enterprises maintains a 24X7 IT Help Desk for support of computer user needs. The Help Desk maintains it's own staffing during normal business hours and rolls back to IT Operations Support after hours. IT Support staff provide in-office response during normal business hours and provide remote support via dial-in VPN connections for after-hours support.

Standard applications are email, office automation products (word processor, spreadsheet, and presentation graphics) and access to the intranet. Any other applications are provided only after an authorized service request has been processed. All applications except office automation require an individual user id for access. Office automation products are configured to save user documents to a protected file server. Intranet access is provided and allows access to the Internet only after authentication with a valid user id and password. Users sign confidentiality agreements in initial orientation and are kept on file with personnel records. All confidentiality agreements are renewed annually and at refresher security training.

Due to the rapid amount of growth and to better service the employee, physician, patient and community information needs, GIAC has also initiated a web presence, www.GIAChospital.com . This initial offering provides a basic, information-only web site. Selections include medical resource information, hospital announcements, job postings, maps/directions, human resources information, medical phone directory and contact information for all departments and specialty programs. The strategic plan for GIAC Hospital has targeted significant development and growth in the Information Technology Department intranet and Internet applications. New applications such as E-health, e-commerce, physician services enabled via the Internet, patient education, patient initiated requests for prescription refills, appointment scheduling, diagnosis specific treatment and communication requests directly from the web site are identified.

Information security management, operations and monitoring have recently been identified as mission critical to enable information based, online solutions.

GIAC Enterprises realized a need for improved security in order to support the rapidly increasing reliance on information systems. GIAC contracted for a vulnerability assessment and penetration test that confirmed those needs. The final report was very beneficial to management's understanding of their current security status.

GIAC has since named a security manager and identified the need for an integrated corporate security policy. They are continuing efforts to mitigate risks identified with the analysis. GIAC is also initiating efforts to provide compliance with the Health Insurance Portability and Accountability Act (HIPAA).

Assignment 2: Define Security Policy

Define Security Policy (50 points) This section is intended to identify areas of particular risk, and define appropriate security policies and procedures to mitigate those risks.

2.1 Assigned Task

Define Security Policy (50 points) This section is intended to identify areas of particular risk, and define appropriate security policies and procedures to mitigate those risks.

Areas of Risk

- Based on the nature of GIAC Enterprises' business, select **five (5)** subjects that represent significant security concerns (i.e., establishing a secure perimeter; security of mobile or remote users; protection of key data; sufficient security awareness/training for users; rapid detection of any intrusions or security breaches; compliance with industry-specific regulations; etc.). Explain:
    - **why** these are areas of particular concern to GIAC Enterprises;
    - **what** the particular threat or risk is;
    - **what** are the possible consequences (loss or damage – material, financial, intangible…) if a vulnerability were successfully exploited;
    - **recommended** steps that can be taken to mitigate the risk.

Security Policy

- For **three (3) of the risk areas** that you identified above, provide a security policy that addresses the risk and takes appropriate steps to mitigate the risk. Your policy should explain the risk it is intended to address, and provide appropriate guidance for mitigating that risk. The policy should be general or high-level, but not completely generic (i.e., no "boilerplate" policies) – it should be tailored to meet the GIAC Enterprises' business and operational structure as described in Assignment 1.

- Your policy should include, at minimum, the following components:
    - **Purpose.** A brief statement of why the policy is being established.
    - **Background.** An optional component which may expand upon Purpose.
    - **Scope.** The extend of the policy – who and/or what is covered by this policy.
    - **Policy Statement.** This section identifies the actual guiding principles or what is to be done. The statement(s) are designed to influence and determine decisions and actions within the scope of coverage. The

statements should define actions that are prudent, expedient, or advantageous to the organization.
    - **Responsibility.** Who is responsible for what. This may include information on who can draft, review, approve, or modify policy; who will carry out specific policy directives; who will ensure that the policy is properly enforced, and so on.
    - **Action.** Specifies what actions are necessary and when they are to be accomplished.

- Note that a given area of concern may need to be addressed by multiple methods. For example, protection of critical data may include securing the data on a server or within a database; securing the data in transit over internal or external networks; ensuring that users who work with sensitive data have appropriate clearances, training, and so on.

2.2 Areas of Risk

These are areas of risk for GIAC Enterprises

2.2.1. Email Virus Risk

Why these are areas of particular concern to GIAC Enterprises.

GIAC Enterprises utilizes email as one of the primary tenants of our corporate strategy to effectively and efficiently maintain communication throughout the company. Each employee is assigned a network logon and email account id during orientation. In addition to basics on how to use the email system, each employee will receive training and practice guidelines on the importance of maintaining confidentiality, privacy and utilizing good security practices. After completing orientation, employees are then allowed and encouraged to utilize email for all internal corporate communication. Most employees will also be allowed to send and receive email over the Internet via the internal email system.

It is because GIAC relies heavily on email as it's preferred method for enterprise wide communication that virus protection / anti-virus policies and procedures are a major concern to the company. Anytime a particular service is identified as a part of the foundation strategy to accomplish a corporate goal, it must also receive equal attention as to how that service will be protected.

What the particular threat or risk is.

If the risk associated with having email at all is acceptable to the corporation, then the major threat to the effective and efficient use of the email system is clearly viruses, trojans, worms and other types of malicious code. These threats which are in a continually evolving state, threaten to disrupt normal communications and therefore to the communication system for GIAC and it's employees. They also represent a danger to the associated computers, networks and computer infrastructure in which the infected machine or message comes in contact with. It is therefore imperative to maintain healthy virus protection / anti-virus policies and procedures to protect against these type negative events.

Any email sent, received or forwarded and the computer used is a candidate for infection and potentially could infect others if a healthy anti-virus strategy is not employed. The virus protection must be multi-tiered to address anti-virus at all levels of infrastructure contact within the organization. The initial virus is normally spread via email so the infrastructure will need anti-virus at several points including the email gateway (interface between the internal email system and the Internet), the mail server and any other server or equipment which may handle, monitor, filter or distribute mail

(including routers and switches), and the end point recipient or end user desktop. In recent cases with some of the newer viruses, the email recipient does not even have to open an attachment to activate the infection.

In addition, an initial infection may occur at any point at which a user will introduce a new file or program to the system. This can be from any removable media such as a diskette or cd or from a download, file transfer, disk sharing or connection to another network. All Internet user accounts are established to not allow downloads or file transfers by default. Only after the proper justification and approvals are received are Internet users authorized for such action. It is also very important that not only the employee maintain good anti-virus practices but everyone they contact or communicate with.

Obviously with all the source points and methods of infection, the important issue is to establish a hardened perimeter that will not allow an infection through. This is not limited to deploying hardware and software to protect against these infections, but to a much larger degree educating users on awareness training and the employment of safe security practices that will minimize exposure to these threats.

What are the possible consequences (loss or damage – material, financial, intangible …) if a vulnerability were successfully exploited.

It is very wise to focus heavily on preventing virus infection, especially with email in the first place. But no matter how good the protection component of your security strategy is, at some point and time in the future you will get infected. The variations of what can happen after an infection are unlimited, so we will try to identify a few of the consequences.

A favorite activity of most email virus infections is to share information with others through use of your email address book. What they share may be any type of information, from what is stored on your PC to any information accessible through your corporate network system. Everything connected to the network can be pictured as a big spider web. A good concept to remember is that everything that is connected electronically can potentially be reached and shared with others. The question to each user is what confidential information do you have access to?

Infections of this nature, which use your address book, can replicate throughout an organization bringing email communications to a halt. The resulting cleanup of such infections can be costly and time consuming.

As a healthcare provider GIAC Hospital has an electronic patient record. It also has integrated the major information systems that include clinical, financial, and laboratory systems. From a clinical standpoint, everything pertinent to the patient, their visit and their care is online. This includes demographic information, insurance information, diagnosis, history and physical information, various clinical assessments, psychotherapy notes, medical procedure information, medical orders for treatment,

prescriptions, doctor notes, laboratory tests and results. From a financial perspective, insurance benefits, authorizations, payment information, account numbers, balance information, beneficiary information, charges and claim status information is accessible. Optical images of insurance cards and drivers licenses are also captured and accessible via the internal network. Probably the most private category of patient information is related to the laboratory system. Medical orders authorizing the tests, the test and the testing procedures themselves, and ultimately the results are available through a connection to this system.

Although GIAC Enterprises is a healthcare provider, you may also have access to confidential information other than patient information. Could it be payroll data, human resources information, finance information, budget, contracts, pricing, fee schedules, etc. that is shared with the world?

Another favorite activity with infections through email is to load and activate malicious software on your PC that can be remotely controlled, unknown to the PC user. These are commonly known as trojans. Like the trojan horse used by the Greeks to gain access to the city of Troy, this software can lie dormant until some trigger causes it to activate. Again these can take multiple forms of payload activity with various resulting consequences. The important point is they allow something else to control what activity takes place on your computer. Anything from information collection and distribution, to destruction of data, stealing resources from your machine, to allowing your PC to be used in an attack against another computer system. The options are endless.

An additional consequence is that either the system or network infected can be made unavailable. This can be the result of a directed attack against GIAC Enterprises, GIAC resources consumed in an attack against someone else, or a general instability in the network itself. In a healthcare environment, it is imperative that our systems be online and available. Even though we have business continuance procedures that allow GIAC to continue operations in the event of system unavailability, it has an operational effect on employees and patients.

An added problem associated with email viruses is they can do damage to the system or it's information. Deleting files which are integral to the operating system functioning on your PC, erasing programs and software, deleting data files (many times on your local drive which may not have been backed up recently – or at all), or physically causing the the system to burn out a component such as a hard drive are all potential results of viruses introduced by email.

Recommended steps that can be taken to mitigate the risk

Corporate steps:

- only connect corporate standardized desktops to the local network. These will include the current release of anti-virus software and current version of anti-virus signatures. These will also not allow end users to modify the configuration of their PC.

- Only allow anti-virus software to be disabled on specific computers when approved by IT Security.
- Auto-start will always start anti-virus software and auto-update current signature files before any user-selected application can be accessed.
- Utilize “push” technology to force update all user anti-virus signature files in emergency situations.

End user steps[2]:

- Insure that the installed anti-virus software is always running
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, this should be specified in GIAC Enterprise’s *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Laptop users should back-up critical data and system configurations on a regular basis and store the data in a safe place.
- In special situations when the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or downloading.
- New viruses are discovered almost every day. Visit the anti-virus software vendor’s web site to monitor current activities.

[2] http://www.sans.org/newlook/resources/policies/policies.htm#template

2.2.2. Security Awareness/Training Risk

Why these are areas of particular concern to GIAC Enterprises.

GIAC Enterprises continues to grow in many new technological areas. Historically, corporate information technology security has been evolutionary and independent. No corporate level security policy existed. Now as GIAC Enterprises begins to expand its services, it will rely on computer systems and technology to a much greater degree.

In order to get from GIAC's current security state where security responsibility only exists in a very limited capacity and totally within the IT department, to a defined corporate baseline level where each employee knows they have a security responsibility every time they see information, will take a major culture change.

GIAC Enterprises can invest vast amounts of money into IT security purposes, but until every employee understands their role with regards to security and takes proactive steps to mitigate the risks, at their level of information interaction, those expenditures will not produce a secure environment. News headlines are full of stories where well-funded, highly complex, integrated IT security architectures are compromised by a worker who doesn't realize that their actions led to a security breach. They are simply unaware of how their actions introduce a weakness into the security structure of such an advanced company. Actions such as selecting "remember my password", writing down their user id and password, using weak passwords, leaving their terminal logged on, all seem very innocent compared with the potential for danger.

GIAC has a corporate responsibility to provide appropriate training and education in a continuing process if they expect their employees to be a security asset rather than a security liability. Automated equipment will continue to function in a reliable manner without retraining and with very little risk of failure. The human element of security always presents the highest security risk because it requires continual training in order to perform in the same fashion.

What the particular threat or risk is.

One risk GIAC should be able to mitigate with minimal effort is the initial training to educate employees to their responsibility in the corporate security scheme. The much harder risk is to keep employees sensitive to the issues of security over prolonged periods of time. Programs which initially do a good job in training must constantly be revised and improved and are challenged with how to continually keep the employee awareness at a heightened level.

Not only are the educational programs a challenge to keep updated and effective, but management must understand the prolonged benefits of training and continue to provide support through enforcement and budgeting.

One additional consideration with regards to IT security awareness training is in the area of new development. Management must allow and appropriate amount of time for development and implementation of training requirements when scheduling and rolling out new technology. On many occasions, an accelerated implementation schedule does so by shortening or eliminating the time allotted for security integration and training.

What are the possible consequences (loss or damage – material, financial, intangible …) if a vulnerability were successfully exploited.

Although in many instances when dealing with security, the consequences are the same (loss of information confidentiality, integrity, availability), there are certain cases where GIAC Enterprises could stand to lose more than at other times. These situations result when the security breach is caused by an insufficient security awareness training program for their employees. It is one thing to have a highly effective training program in place where the employees are well aware of the consequences and are given information and opportunity to participate in protecting the organization, but is beaten by a superior challenger. It is quite another issue, when the perception or reality is that GIAC did not provide what was needed in either funding or basic security education to properly prepare their employees.

GIAC Enterprises prides itself on being a community leader in healthcare with tremendous patient loyalty. If the headlines of tomorrow's news reported a security breach, that possibly would have an impact on patient selection of GIAC for a limited amount of time, and therefore a slight financial impact on revenue. If those same headlines indicate that GIAC was at fault for not providing sufficient security training for employees, this could do irreparable damage to their credibility, result in loss of established market share, increase cost to recruit new patients, reduced the success of future programs and possibly expose the company to additional liability.

Any of these actions will have long-term impact and a greatly increased impact on revenue. Depending on the severity of a breach and the perceived amount of negligence for inappropriate training, GIAC could be identified as not providing due care and potentially be at risk for regulatory accreditation. The consequences of being compromised are bad enough by themselves. However, it could get worse if patients not only lose confidence in GIAC's ability to keep information secure, but also lose faith in our ability to provide quality healthcare.

Recommended steps that can be taken to mitigate the risk

- Establish and assign responsibilities for all access levels (IT Secure Access, Help Desk Support, End Users, etc.) of security awareness training to the IT Security Department
- Assign all security issues (including training) to the Information Security Officer
- Insure an adequate budget for security awareness education and training

- Provide variations in housewide security training options based on learning preferences of users (computer based, written format, classroom instruction, video tape, interactive intranet, etc.)
- Require initial security awareness training during orientation and with annual continuing education requirements.
- Require certification testing of employees annually.
- Do not tie information security awareness to computer systems only. Security responsibility for information occurs regardless of the sensing or media (spoken, heard or seen in oral, written, printed, faxed, or electronic format).
- Include security status statistics and incident information in all levels of regular management reporting.
- Continually include security awareness tips and information in all corporate communication forums (weekly corporate bulletins, GIAC monthly educational television, regular housewide emails, etc.)
- Insure awareness training and communications exists for off-shift employees
- Develop 30 second info-mercials on a variety of security subjects
- Define security requirements and training and require for all new system installs
- Define security requirements and training for legacy systems

2.2.3. Centralized Information Security Management Risk

Why these are areas of particular concern to GIAC Enterprises.

As GIAC Enterprises continues to develop new programs and facilities for it's patients and employees, it also increases it's reliance on information technology. This dependence on information availability and the delivery computer system infrastructure also creates a critical need to organize, coordinate, integrate and manage all information security from a centralized area of responsibility. GIAC needs to establish a centralized management area that has the responsibility for all information security (ITSec). ITSec should be responsible for establishing the corporate baseline security requirements, implementing policies & procedures and security operations to insure the organization is in compliance with those requirements. This area should report to the CEO level of GIAC Enterprises. If direct reporting to the CEO is not possible, at a minimum the area should report to the CIO level and directly be responsible to the CEO.

The extremely important and complex task of information security is ineffective unless managed from a single area of responsibility. ITSec should represent all technical areas in which security responsibility falls. The currency, width and depth necessary of this broad range of security subject areas can only be provided by a community of security specialists. The GIAC current level of security is evolutionary and totally dependant upon the IT implementation team for the project without concern for an overall integrated security scheme. Any non-system security issues are addressed independently outside of IT. This does not serve the security requirements for GIAC.

What the particular threat or risk is.

The overriding principle here is that a security risk accepted by one is forced upon all. Without a centrally organized and integrated security plan, a piecemeal approach with potentially opposing security stances creates very open and vulnerable information systems. Major security breaches in today's environment are many times the result of a very slight oversight in the coordination, integration, or implementation of a very qualified security plan. Imagine how easy a compromise becomes when the security policy is not a tightly woven, seamless integration utilizing defense in depth principles.

The visual image is that of a very weak protection mechanism, full of holes and incapable of providing any security for the organization. In addition, once a security breach has happened, without a central authorized management area, appropriate incident response and recovery is virtually impossible.

Modern day security threats can come from virtually anywhere with a multitude of motivations. Hackers, disgruntled ex-employees, vandals, corporate espionage, script kiddies, extremists and information abusers are all sources of security compromise and can target GIAC Enterprise systems for any number of reasons. These attacks can be

launched from inside or outside the organization, at any time of the day or night, and from virtually anywhere in the world.

What are the possible consequences (loss or damage – material, financial, intangible …) if a vulnerability were successfully exploited.

One of the consequences of not having centralized security management is that intrusion is easier and discovery is less likely for longer periods of time or possibly ever. An intruder can simply fall through the cracks and depending on how many of those cracks are aligned may well determine the level of compromise that is achieved. Without continued refinement and review normally managed by IT Security, the hole or breach may remain and continue to be exploited in the future.

Although the normal results of poor security are very undesirable, many times the effects are immediately known and addressed. Delayed detection and usually results without a centralized IT Security Management Area. These long-term effects may be the wholesale theft of complete information repositories over time from corporate systems. These can be databases of credit card numbers, patient medical records, and proprietary client lists. Breaches of this nature are usually very malicious, cause tremendous embarrassment and result in extremely high financial impact. In many instances the organization cannot recover from the damage done to their credibility and for many years, if they remain operational, continue to suffer from the incident.

Not only does the organization have to deal with the effects of the incident once it is realized, it must try to identify and eliminate the vulnerability that was used. This is almost impossible without a dedicated centralized security area of responsibility. A favorite ploy used recently by hackers to prove their exploits of well-known and respected organizations is to post the results of their work publicly. A challenge or demand is then issued to the compromised company to find the hole and make changes or they will continue to suffer at the hands of the attacker. This is the modern day example of gunfighters dueling in the streets at high noon.

Again, with all the consequences of normal security exploitation there is the added impact on the patient you are trying to serve. They may be asking themselves if GIAC Healthcare can't even protect my information that may not physically do me harm, how much can I trust them with my health care that could potentially cost me my life?

Recommended steps that can be taken to mitigate the risk

- Establish a corporate IT Security Department who is responsible for all facets of information security operations
- Assign the information reporting structure to the CEO and the physical reporting structure to the CIO at a minimum
- Establish a Security Task Force from the community of IT resources who are responsible for the implementation of security on the information infrastructure.

- Define as a responsibility of ITSec that current industry knowledge must be maintained and budget accordingly
- Mandate that an audit policy requiring annual review must be a part of standard documentation for all systems

2.2.4. Industry Guidelines Compliance Risk

Why these are areas of particular concern to GIAC Enterprises.

GIAC Hospital is an accredited facility with the Joint Commission on Accreditation of Healthcare Organizations (JCAHO). JCAHO's purpose is "to continuously improve the safety and quality of care provided to the public through the provision of health care accreditation and related services that support performance improvement in health care organizations. "[3]

> JCAHO standards require that organizations strive to continuously improve the services they provide and examine systems and processes for risk factors that may lead to medical errors and sentinel events… The Joint Commission's accreditation process seeks to help hospitals identify and correct problems and improve the safety and quality of care and services provided.

Passing or receiving accreditation assures the community that the facility has met stringent guidelines in all areas of healthcare operations. The scoring mechanism with the accreditation also provides an opportunity to compare GIAC Enterprises against other JCAHO facilities.

Without an independent accreditation like JCAHO, GIAC Hospital will be unable to qualify for contracts to provide healthcare services for many insurance companies and Medicare / Medicaid services. Therefore it is tremendously important to insure not only a passing grade but also receive a high score.

GIAC Enterprises will be legally mandated to comply with an even more extensive set of rules and regulations beginning in October 2002. The Health Insurance Portability and Accountability Act (HIPAA), enacted by Congress on August 21, 1996, will require a fully integrated information security methodology.

> HIPAA requires the promulgation of standards on how health care providers, health plans, health care clearinghouses, employers and third-party entities that furnish health care services or supplies transmit and store health information in electronic form. The security standards apply to any health information pertaining to an individual that is electronically maintained or transmitted. They require health care entities to implement technical, administrative and physical security measures. [4]

Failure to comply with the security standards can result in civil fines, criminal penalties and criminal fines.

---

[3] © 2001 by the Joint Commission on Accreditation of Healthcare Organizations, http://www.jcaho.com/trkgen_frm.html

[4] http://hipaa.ascensionhealth.org/overview/introduction.html

What the particular threat or risk is.

With the stringent requirements of both JCAHO and HIPAA, GIAC Enterprises will have to very quickly institute an enterprise wide, integrated information security system. The JCAHO accreditation will insure very basic information security processes are in place and maintained with ongoing quality control processes at GIAC. HIPAA has legislated very specific requirements guaranteeing that a much higher level of information security exists. Both are geared toward providing quality, security benefits to the patients, the provider organization and the entire healthcare community.

These requirements do not just simply identify a laundry list of selectable, independent security implementations that will satisfy a checklist. They are requiring full-fledged integrated security, complete with changes to overall operational procedures that compliment and support these changes. In essence, a complete turnkey security installation is mandated within a very short timeframe - considering the vast impact these changes require. JCAHO requires surveys be completed every three years. HIPAA legislates specific dates by which security changes must be made. These begin as early as October 2002.

An additional risk exists with HIPAA compliance as the deadline dates have already been established. Like many other healthcare providers, GIAC has not yet begun and the deadline is already approaching. Because this regulatory requirement is due at the same time for the entire healthcare industry, resources for outsourcing will become very limited in a very short period of time.

What are the possible consequences (loss or damage – material, financial, intangible …) if a vulnerability were successfully exploited.

It is a given that failure to meet either JCAHO or HIPAA security regulations will put GIAC Enterprises at significant risk as both of these provide methods of enhancing information security within the organization. However, there are significant consequences other than just having poor security and all the problems that can cause.

Failure to receive JCAHO accreditation will cause GIAC Hospital to loose contracts with many commercial insurance companies, not to mention federal healthcare contracts such as Medicare and Medicaid. This would severely impact hospital revenue due to the loss of patient volume, as GIAC would no longer be an acceptable provider to most insurance plans. If accreditation was received but with a low passing score, similar results could result if insurance carriers require scores higher than simply passing. In addition, a low score could be targeted in an advertising campaign by competitive institutions thus potentially losing not only revenue dollars but reputation and patient loyalty.

Failure to meet HIPAA regulations falls into a different consequence category because law mandates them.

> Failure to comply with these regulations may result in civil fines of up to $25,000 for multiple violations of the same standard in a calendar year. However, if a failure to provide adequate security results in a misuse of individually identifiable health information, additional criminal penalties may be imposed. Depending on the degree of criminality fines range from $50,000 to $250,000 and imprisonment from one to ten years.[2]

Note: HIPAA regulations are stricter and more encompassing than JCAHO standards and will provide for compliance with JCAHO.

Recommended steps that can be taken to mitigate the risk

- Perform a gap analysis as soon as possible between any existing security and HIPAA regulations and develop a compliance workplan (compliance with HIPAA will provide for compliance with JCAHO, see note above).
- Start now with known tasks. Before the results of the gap analysis are delivered, there are many known tasks that can be started.

Because the deadline for compliance has already been established and this requirement affects every component of the healthcare industry, the time frame for beginning these steps is crucial:

- Immediately form a corporate level HIPAA Steering Committee with reporting responsibility to the CEO
- Immediately establish HIPAA compliance as a corporate priority and dedicate sufficient budget and resources to the project
- Immediately identify a Security Officer and a Privacy Officer as required by HIPAA
- Immediately begin compiling complete and accurate inventories of policies and procedures, software systems, data classification by system, information flow documentation and business partner contract information.
- Immediately have legal departments begin identifying the “official” GIAC Enterprise interpretation of the regulations.

[2] http://hipaa.ascensionhealth.org/overview/introduction.html

2.2.5. Risk of Weakened Passwords Due to Number of User Ids

Why these are areas of particular concern to GIAC Enterprises.

Password entry is the security methodology used to authenticate the person utilizing a particular user id. The weaker the password the weaker the defense mechanism provided by user authentication. When a single user must utilize multiple ids on a daily basis in their normal job responsibilities, the challenge of continually maintaining a scheme for creating strong passwords can make the effort very difficult.

What the particular threat or risk is.

The GIAC Enterprise password policy suggests users utilize different strong passwords for each user id. Considering that a typical GIAC user will have to authenticate to the network, email, Internet, and at least one application system, the probability is high that over time, users will either reuse passwords with multiple systems or choose weaker passwords overall.

In addition some systems (normally older legacy systems) do not have the capability to enforce strong password syntax or acceptable change frequency. GIAC Enterprises does not have the ability to monitor passwords across systems or applications.

Once an unauthorized user is inside using a valid user id, they are camouflaged from detection and can increase their level of malicious activity with a tremendously reduced chance of being caught. They may be able to install software so that with each succeeding password change, they are automatically notified.

Also, once the effort required to comply with policy exceeds the effort for non-compliance, the risk is much greater that the policy will no longer be complied with.

What are the possible consequences (loss or damage – material, financial, intangible …) if a vulnerability were successfully exploited.

Once password strength is weakened, even for a single user, a number of consequences are now possible. These include the ability for passwords to be compromised with less effort, automatic user id lockout features are not as effective and "low and slow" attacks are more effective. If the same password is used across multiple systems, once a single password is cracked then other systems can be accessed with little or no effort. If the change frequency is reduced then an unauthorized user can continue to access the system for longer periods of time without the risk of being discovered.

After an unauthorized user begins using a valid password, detection becomes almost impossible unless the user violates another security policy and triggers a security

notification. In addition, recovery becomes impossible because there is no way to distinguish between authorized and unauthorized activity.

Recommended steps that can be taken to mitigate the risk

As long as key entry of passwords continues:

- Provide regular awareness training on the importance of maintaining strong passwords
- IT Security should regularly run password-cracking software to audit the strength and compliance of passwords with password policy. These operations should only be completed in accordance with strict procedures which detail who is authorized to run this software, at what times, what notifications are required prior to running (as these tools can be very resource intensive and have system impact), required actions when a password is identified as non-compliant and resulting actions to users who continue to violate policy.
- Install password management software

A two-staged authentication process can be added to greatly reduce the risk associated with a single authentication process.

Install a “military grade” biometric fingerprint scanner that will replace the user id/password entry at all levels. These scan devices utilize upwards of 70 minutia points per fingerprint thus providing a much stronger authentication process than weaker scanners or password entry.

2.3 Security Policy

These are GIAC Enterprises Security Policies.

2.3.1. Anti-Virus Policies

These are GIAC Enterprises Security – Anti-Virus Policies

2.3.1.1. Virus Protection Strategy Policy

Purpose.

This policy defines the requirements for deploying, maintaining and executing the virus protection strategy at GIAC Enterprises.

Background.

Because both email and proper desktop functionality is such an integral part of corporate communications at GIAC Enterprises, virus protection must be actively running at all times and in accordance with the anti-virus strategy.

Scope.

This policy covers installations of all software used in maintaining the virus protection strategy at GIAC Enterprises. This includes the virus definition update server, email gateway, application & file servers and desktop PCs connected to the network at GIAC Enterprises.

Policy Statement.

The virus definition server must continuously run an automated script that will access the anti-virus software vendor site **every hour** and download any available updated signature files. If found, the updated signature files must then immediately be pushed to the email gateway, then to all application & file servers and then to all desktop PCs.

The approved corporate version of anti-virus software must be continuously running on the email gateway, all application & file servers and all PCs connected to the network.

Although special situations may exist whereby virus protection must temporarily be disabled at the desktop, the intent is to reactivate the software as soon as possible to continually provide protection against the transportation and activation of malicious software at any point on the GIAC Enterprise network.

Responsibility.

It is the responsibility of IT Virus Administrator to maintain the automated script on the virus definition server and insure it is constantly running.

It is the responsibility of IT Server Support for testing, maintaining and deploying the approved corporate version of anti-virus software on the email gateway, application & file servers and desktop PCs. New releases of anti-virus software should be deployed as soon as possible after they have been tested and deemed production ready.

Users who are approved to temporarily disable virus protection software at their desktop must follow specific procedures provided by IT Security and are responsible for reactivating the software immediately after the situation requiring deactivation has ended.

It is the responsibility of IT Security to:

- Provide desktop user training on how to properly disable and enable the installed anti-virus software.
- Provide housewide training on how to report problems or suspicious activity with PC hardware.
- Maintain and review this policy
- Audit for compliance with this policy.

Action.

Violations of this policy should be reported to the Corporate Security Hotline.

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

2.3.1.2. Desktop / Laptop Anti-Virus Policy

Purpose.

This policy defines the requirements that must be met by all desktop and laptop computers connected to GIAC Enterprises network to ensure effective virus detection and prevention.

Background.

Because viruses are normally introduced to the network from the desktop level, anti-virus software must be actively running on desktop and laptop computers at all times and in accordance with the anti-virus strategy.

Scope.

This policy applies to all desktop computers connected (or which are capable of connecting) to the network at GIAC Enterprises. Desktop computers include, but are not limited to, all computers issued to employees or those that are used by employees to connect to the network, including laptops.

Policy Statement.

All GIAC Enterprise desktop computers must have the approved corporate version of anti-virus software installed and running at all times. The anti-virus software and the signature update files must be kept up-to-date.

Virus infected computers must be removed from the network until they are virus free. Any activities with the intention to create and/or distribute malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) into any PC or network (belonging to GIAC Enterprises, any other company or any individual) are prohibited, in accordance with the GIAC Enterprise's *Acceptable Use Policy*.

Refer to GIAC Enterprise's Anti-Virus Recommended Processes to help prevent virus problems.

Exception: in special situations users may temporarily disable the anti-virus software program. However, they are to only do so using IT Security issued guidelines and are responsible for immediately reactivating the software once the situation requiring deactivation has ended and before resuming any other activity.

Responsibility.

It is the responsibility of IT PC Desktop Support to insure every desktop computer issued is configured using the current standard security configuration which includes anti-virus software and up-to-date virus definition files.

It is the responsibility of IT Server Support to provide the up-to-date virus definition files for Desktop Support.

It is the responsibility of every desktop user to insure that the installed anti-virus software is running.

It is the responsibility of IT Security to:

- Provide desktop user training on how to properly disable and enable the installed anti-virus software.
- Provide housewide training on how to report problems or suspicious activity with PC hardware.
- Maintain and review this policy.
- Audit for compliance with this policy.

Action.

IT Security will audit the entire virus definition update process on a semi-annual basis.

Violations of this policy should be reported to the Corporate Security Hotline.

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

2.3.1.3. Anti-Virus Scanning Requirements Policy

Purpose.

This policy defines the anti-virus scanning requirements for GIAC Enterprises.

Background.

Because of the impact to operations and potentially to the delivery of care once a virus infection has begun, GIAC Enterprises prescribes where anti-virus scanning, at a minimum, must take place.

Scope.

This policy identifies the location and types of anti-virus scanning which must take place on the GIAC Enterprise network.

Policy Statement.

Email Gateway
All email messages and their attachments down to 12 levels deep coming from outside GIAC Enterprises will be scanned with the current signature file before being transferred to the internal mail system. In addition, any attachments with file extensions matching the current File Extension Block List will be stripped and replaced with the standard security notification attachment.

Communications Servers
All outside emails with attachments will be scanned before being delivered. Those found with file extensions matching the current File Extension Block List will be stripped and replaced with the standard security notification attachment then delivered.

Desktop Computers
All desktop computers will continuously run the installed anti-virus software and scan all outside email with the current signature file before being delivered to the mail application. In addition, the targets of all file activities (open, save, execute) will be scanned before being allowed to process. Any virus detection at this point will notify the user with an error message to the screen and not allow the file operation to process. The IT Anti-Virus Administrator will also immediately be sent a notification message.

Responsibility.

It is the responsibility of IT Server Support to insure that anti-virus scanning takes place on the email gateway and application & file servers.

It is the responsibility of IT PC Desktop Support to insure that anti-virus software is installed and configured to scan on the user desktops.

It is the responsibility of every desktop user to insure that the installed anti-virus software is running.

It is the responsibility of IT Security to:

- Provide desktop user training on how to check the activity status, properly disable and enable the installed anti-virus software.
- Provide housewide training on how to report problems or suspicious activity with PC hardware.
- Maintain and review this policy.
- Audit for compliance with this policy.

Action.

Violations of this policy should be reported to the Corporate Security Hotline.

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

2.3.1.4. GIAC Enterprise's Anti-Virus Recommended Processes

These processes are recommended to help in the prevention of virus problems:

- Insure that the installed anti-virus software is always running
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with GIAC Enterprise's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- In special situations when the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or downloading.
- New viruses are discovered almost every day. Visit the anti-virus software vendor's web site to monitor current activities.

Adopted from SANS Security Policy Project[6]

[6] http://www.sans.org/newlook/resources/policies/policies.htm#template

2.3.2. Industry Guidelines Compliance Policy

Purpose.

The purpose of this policy is to identify and set expectations for compliance with industry regulations and guidelines.

Background.

Basic information security is important to GIAC Enterprises. It is also important to GIAC in our ability to comply with accreditation standards established by Joint Commission on Accreditation of Healthcare Organizations (JCAHO). Those basic standards are included as well as significantly increased privacy and security components now mandated by law with the passage of the Health Insurance Portability and Accountability Act (HIPAA).

Scope.

This policy applies to all GIAC Enterprise employees, medical staff, contractors, consultants, temporaries, students, volunteers and other personnel and companies affiliated with GIAC. This include Business Entities and Business Partners associated with GIAC as defined within HIPAA.

Policy Statement.

General
The activities of GIAC Enterprises and associates should always be in full compliance with legal regulations at all times.

Specific to Information Management
GIAC Enterprises and associates should always be in full compliance with the quality and performance improvement standards established by JCAHO, especially those involving management of information (IM).

GIAC Enterprises and associates should always be in full compliance with the Transaction Set, Privacy and Security standards mandated by law as specified in HIPAA. Although neither JCAHO nor HIPAA are repeated here, compliance with those specific policies and procedures are a part of this policy.

It is also understood that both JCAHO and HIPAA are living specifications and are constantly maintained and updated. Compliance is interpreted as meaning the current version of the requirements as approved by GIAC.

Responsibility.

It is the responsibility of every GIAC Enterprise employee and associate to insure this policy is being complied with or reported to the Corporate Compliance Hotline.

It is the responsibility of the identified JCAHO and HIPAA named administrative personnel to review and make any necessary changes to this policy annually (JCAHO Compliance Administrator, HIPAA Privacy Officer, HIPAA Security Officer).

It is the responsibility of IT Security to maintain and review this policy; and audit for compliance with this policy.

Action.

Violations of this policy should be reported to the Corporate Security Hotline.

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

2.3.3. Security Awareness/Training Compliance Policy

Purpose.

The purpose of this policy is to provide general guidelines for Security Awareness and Training of GIAC Enterprises employees in order to improve both individual employee performance and organizational performance in compliance with JCAHO standards and HIPAA regulations.

Background.

GIAC Enterprises has a basic belief that knowledgeable employees are better overall employees and will train easier if they have a goal of educating for a specific purpose. GIAC has a corporate responsibility to provide appropriate training and education in a continuing process if they expect their employees to be a security asset rather than a security liability. The human element of security always presents the highest security risk and requires continual training in order to perform according to expectations.

Scope.

This policy applies to all GIAC Enterprise employees, medical staff, contractors, consultants, temporaries, students, volunteers and other personnel, and companies affiliated with GIAC. This includes Business Entities and Business Partners associated with GIAC as defined within HIPAA.

Policy Statement.

All personnel are required to be trained in Security as it relates to the management of information. This will include general knowledge as well as security training requirements in compliance with JCAHO and HIPAA. This training will be incorporated into the established programs of the GIAC Enterprise Education and Training general policy. The general education is provided in the following categories:[7]

- Employee Orientation
- Continuing Education
- Competence Evaluations

Employee Orientation will include the GIAC Enterprise Security Immersion Training as prepared and provided by IT Security. This training gives a broad understanding into the general principles of security as well as specific training of all applicable IT Security Policies and Procedures (e.g., computer resources use, confidentiality agreements,

[7] [editedname], Inc. Human Resources Policies and Procedures Manual, 2001

user id issuance, password policy, etc.). This training is certification based and the attendee must pass a test prior to completion.

Continuing Education will include all communication forms used by GIAC Enterprises to disseminate information throughout the corporation. Security Awareness information is included in but not limited to the weekly bulletin (available in printed and email), specific advisories (normally regarding viruses and information security alerts), education seminars, online educational TV, email, computer based training modules, employee safety fair format, special meetings, mandatory monthly departmental staff meetings, intranet and the Internet. They may be delivered as bulletin articles, research papers, videos, table tent reminders, skits, bulletin board education and special promotions.

Continuing Education will also include both housewide and department specific training required annually by JCAHO and HIPAA. Depending on the purpose, immediate importance and impact, Continuing Education training may require certification testing.

Competence Evaluations are conducted by GIAC Enterprise departments and required for all personnel in conjunction with the 90 day and annual performance appraisal. All competency checklists and appraisals must be forwarded to Human Resources for the employee's personnel file.

Although Competency Checklist development is the responsibility of the evaluating department, the Security Awareness component is defined by IT Security and is a mandatory element.

Responsibility.

It is the responsibility of all GIAC Management to insure that Security Awareness Training and Education is provided and understood by all personnel.

It is the responsibility of all GIAC personnel to posses and utilize the knowledge provided in the training in the performance of their job duties.

It is the responsibility of IT Security to develop and maintain all Security Awareness Training and Education.

It is the responsibility of Human Resources to insure that Security Awareness Training is provided during orientation and is included in the annual employee performance appraisal and departmental competency checklists.

Action.

Violations of this policy should be reported to the Corporate Security Hotline.

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

Assignment 3: Define Security Procedures

3.1 Assigned Task

This section is intended to use existing policy to develop operational procedures that can be used to implement and enforce that policy.

For **one (1) of the security policies** that you defined in Assignment 2, create a procedural document that describes how the policy should be implemented.

The procedural document should include information on:

- **what** actions should be carried out;
- **why** those actions are important;
- **who** is responsible for carrying out those actions;
- **when** and/or **where** the actions should be taken;
- **how** you can check or test that the actions have been performed and are having the desired effect (i.e., policy is being implemented and is working as intended).

3.2 Security Procedure

This are the GIAC Enterprise Security Procedures.

3.2.1. Anti-Virus Procedure

This are the GIAC Enterprise Security - Virus Protection / Anti-Virus Procedures.

3.2.1.1. Virus Definition Server Update and Push Procedure

what actions should be carried out;

This procedure identifies the steps necessary to update the definition files on the Virus Definition Server and push those updates out to the email gateway, application & file servers and desktop computers in compliance with the Email Virus Strategy Policy.

why those actions are important;

It is extremely important that this procedure be completed fully, on a regular schedule and in a time sensitive fashion. As new viruses appear almost daily, existing viruses reappear, and smart viruses continually “morph” themselves in an effort to avoid detection, virus protection is a constantly moving target and the landscape can

completely change in a matter of hours. Many recent viruses have been able propagate themselves to the extent that they achieve worldwide distribution with very destructive consequences in a matter of hours. For this reason it is vitally important to have a fast and efficient mechanism for recognizing and distributing virus definition updates as soon as they are available.

who is responsible for carrying out those actions;

IT Security / Anti-Virus Administration is responsible for insuring that the automated scripts and procedures function properly.

IT Operations is responsible for insuring that the scripts are continually running.

when and/or where the actions should be taken;

The automated script on the Virus Definition Update Server should continuously be active. This script(s) will cause the server to go out to the anti-virus software vendor web site and check the GIAC internal signature file against the vendor's current signature file one time every hour.

As soon as the update completes, the script should automatically activate a process on the Virus Definition Server to update or "push" the signature file onto the email gateway, then the application & file servers and then the desktop computers in this priority sequence.

Should any portion of this procedure fail, IT Security should be notified immediately with a priority response status.

how you can check or test that the actions have been performed and are having the desired effect (i.e., policy is being implemented and is working as intended).

The run status on the console of the Virus Definition Update Server should be checked for any errors as a daily task on the IT Operations production schedule.

As an audit check, the email gateway, application & file server and desktop computer anti-virus software should be set to automatically check for how many days since the last update. If the days since last update are ever more than 1 day, the anti-virus administrator should be automatically notified.

Procedure

This is the procedure for updating virus definition files on the Virus Definition Server.

1) Configure anti-virus server to live update every hour.
2) Automate live update process using automated scheduler
3) Configure anti-virus server to push anti-virus updates to email gateway, application & file servers, and desktop computers.

This is the procedure for checking the scripts to insure they are running.

1) Access the Anti-virus console on the Virus Definition Server
2) Access the anti-virus software
3) Click on Histories / Event Log

3.2.1.2. Desktop Procedure for Checking Run Status / Starting / Stopping of Anti-Virus Software

what actions should be carried out;

This procedure identifies the steps necessary for a user to check the run status, start and stop execution of the anti-virus software from a desktop computer.

why those actions are important;

It is GIAC Enterprise's policy for the installed anti-virus software to run at all times. Only in special circumstances and when approved by IT Security can the software be disabled from running. Once the special circumstance has terminated, the anti-virus software must be restarted before any other activities may be begin. It is the desktop user's responsibility to successfully perform these actions in order to comply with the Desktop Anti-virus Policy.

who is responsible for carrying out those actions;

It is the responsibility of the desktop user to insure that these procedures are successfully completed.

when and/or where the actions should be taken;

These procedures should be completed anytime the desktop user desires to check the status, start or stop the anti-virus software.

how you can check or test that the actions have been performed and are having the desired effect (i.e., policy is being implemented and is working as intended).

You may audit the procedure by using the actual procedural steps themselves.

Procedure

For Checking the Status or Starting or Stopping the Anti-virus software:
1. The desktop computer must be booted up and running.
2. Locate the anti-virus software icon in the system tray in the bottom right corner of the screen. If you are not familiar with the icon images, hovering the curser over each icon will display the application name the icon represents.

Checking the Status
1. If the icon has a red circle around it with a line through it, the application is disabled and not running.

2. If the icon does not have a red circle around it with a line through it, the application is running.

Starting / Stopping the Anti-virus Software

1. Right click once the cursor is over the anti-virus icon, a pop-up window will appear with the available options displayed based on the current activation status (if disabled only enable will display, if enabled only disable will display).
2. Highlight the desired option (left click).
3. Press enter.
4. If the icon displays the desired status, you are finished. If the icon does not display the desired status, try the steps again. If the icon still does not display the desired status, contact the IT Help Desk.

3.2.1.3. Desktop Imaging Procedure

what actions should be carried out;

This procedure defines the steps necessary to configure a desktop pc (including laptops).

why those actions are important;

The successful completion of this procedure is important to insure the desktop / laptop computer is configured in compliance with the GIAC Enterprise Secure Configuration Definition Standard. This will assure the computer does not initially present a security risk when installed or when connected to the network.

who is responsible for carrying out those actions;

It is the responsibility of PC Support to complete this procedure.

when and/or where the actions should be taken;

It is required that this procedure be completed before a desktop or laptop can be installed or connected to the GIAC Enterprise network.

how you can check or test that the actions have been performed and are having the desired effect (i.e., policy is being implemented and is working as intended).

An imaged pc does not allow user configuration changes. If it is suspected that modification have been made to the desktop, the Desktop Imaging Procedure should be repeated.

Procedure

1) Connect the physical components of the computer, and power on to insure all connections are recognized. Do not enter name or IP number.
2) Select the version of the ghost image boot diskettes that matches the physical specifications and current operating system (i.e., Dell Optiplex GX240, Win2000).
3) Reboot desktop from the selected ghost image boot diskettes
4) Run Ghost Image Software and select image from the Ghost Server.
5) Remove image diskettes and reboot desktop.
6) Insure desktop connects to the appropriate network, the email application functions (if appropriate) and that the applications can print.

List of References

http://hipaa.ascensionhealth.org

http://www.jcaho.org

http://www.sans.org/newlook/resources/policies/policies.htm#template

http://www.[editedname].com/about/about.html

Wood, Charles Cresson CISA CISSP, Information Security Policies Made Easy, Version 7, Sausalito: Baseline Software Inc., 1999. 146 - 153

HIPAA Training Handbook for the Healthcare Staff: An Introduction to Confidentiality and Privacy under HIPAA, Marblehead: Opus Communications, 2001

[editedname], Inc. Human Resources Policies and Procedures Manual, 2001