Global Information Assurance Certification Paper

GIAC Enterprises
GIAC/ME

ISO Assignment 1.2

Author: John Franco
Date: 09/19/2002

Summary –

It is my attempt to cover all the required assignments for the GIAC ISO certification. I have chosen to use a fictional company in my paper. This is a family owned and run medical office. While they do have several computer networks within their offices, and for a small business they have some expensive hardware. They do not full have an office that would pass the HIPAA regulations for security. My paper will focus on creating a secure environment for GIAC/ME.

Assignment One

Description of GIAC Enterprises

GIAC Enterprises is a family business started by three brothers and their sister in 1950. The brothers, Giovanni, Anthony, Ignatius and their sister Cleopatra came from a very close family. Their parents Nicole and Assunta Conti came over from Italy in the 1930's. Wanting the best for their children, they worked all sorts of jobs and managed to put all four of their children through college. Giovanni and Cleopatra continued with medical school, Anthony became a pharmacist and Ignatius a nurse.

The brothers and sister started off their medical practice in a small town of Bloomfield, New Jersey, naming the practice Gevontie, Anthony, Ignatius, and Cleopatra Medical Enterprises (GIAC/ME). Pooling all their talents and resources they were able to provide affordable medical services to the community. GIAC/ME provides medical services to all and no one was tuned away because of their inability to pay. Eventually GIAC/ME opened a free clinic that provided for the medical need of the community.

GIAC/ME five departments:

- Pediatric Center (GIAC/PC) - a full service pediatric center caring for the full medical needs of newborn to age 18 years old.
- Adult Services(GIAC/AS) care for the young adult through geriatric
- Free Clinic (GIAC/FC) – provides free medical services to those that can not afford it.
- Pharmacy (GAIC/PHR) – Provides a full service pharmacy with discounts to current patients.
- Admin Office - Provides administrative staffing for the other departments, including IT, payroll, accounting services, and patient appointments.

GIAC/ME really cares about their patients and their community. GIAC/ME provides patients with web access to their appointments and provides web access to a complete medical library allowing patients and others to research aliments that they may have. GIAC/ME believes that an informed patient helps with their diagnosis and recovery.

Description of IT Infrastructure

GIAC/ME maintains several databases to assist the staff in caring for the patient. The information in these databases contains among other things the entire patient record, insurance information and other pertinent information for caring for the health of each patient. The confidentiality, integrity and availability of this data is not only important to the GIAC/ME, but there are Federal regulations including Health Insurance Portability and Accountability Act (HIPAA) of 1996. This data must be protected. Please see http://cms.hhs.gov/hipaa or http://www.sans.org/newlook/resources/policies/policies.htm#HIPAA for an explanation of HIPAA rules.

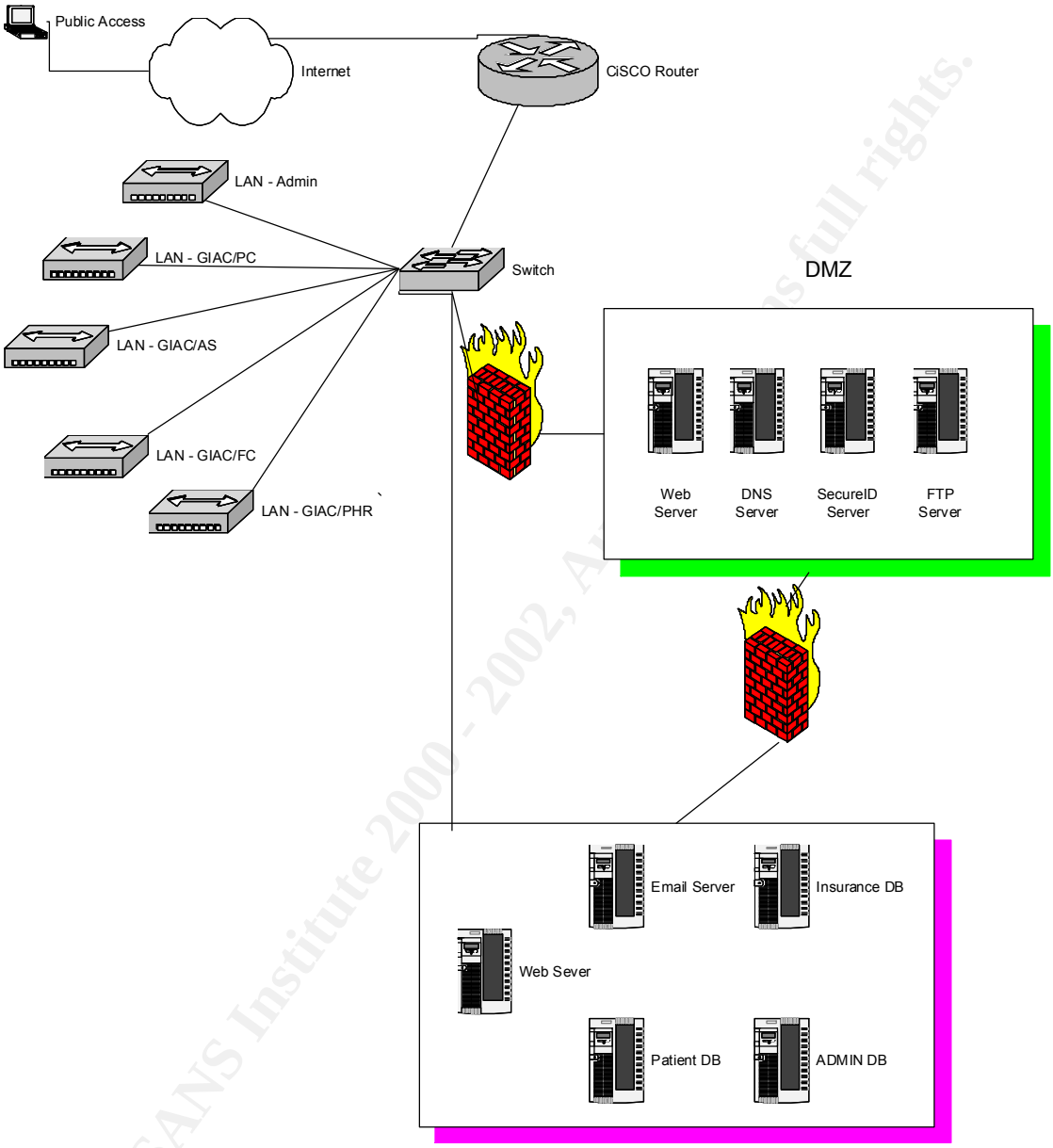
GIAC/ME contracts with Somerset Internet Provider for internet access from their Bloomfield office. The office has a network core consisting of a CISCO 1760 Modular Access Router, Cisco Catalyst 2926 Multilayer Switch, and for security a Cisco IOS Firewall. See Cisco references at the end of this paper

GIAC/ME provides medical information to the community through their website where a user can read and download medical papers and journals. Patients can also view their appointments and even view their medical expenses. In order to protect the patient's data and to protect the office a DMZ was created to protect the databases and servers.

Each department has its own LAN which connects to the switch for both internet and intranet access.

For added security GIAC/ME has RSA SecurID server where the physician and other professionals who need access to the patient data base can access it from outside of the office. http://www.rsasecurity.com/products/securid/index.html and http://www.winnetmag.com/Articles/Index.cfm?ArticleID=26315&pg=4

Figure 1 – GIAC/ME Network Diagram



Business Operations

Caring for the patient is the main focus of GIAC/ME. It is the sole purpose for its existence. The Conti family has a strong sense of community and that is reflected in their organization.

In the GIAC/ME data center there are several databases that contain the complete patient record, patient appointment scheduling and insurance information. In addition to these critical databases, there are servers used for Web and FTP hosting, accounting systems, and an email server. Protecting these databases and servers and ensuring that they are always available is essential to the successful operations of GIAC/ME. Security of these databases and servers is critical and those systems must be protected.

Primary access to these systems is from within the office itself. Each department has access to all the databases and servers. Each user has a single sign-on that allows them only to access the information that they have authority for. For example, an appointment clerk can only access the appointment records, the physician and nursing staff have access only to those patients that are under their care.

Many times the physicians will need to access patient information from outside the office. To enable them to have a secure connection from any location the addition of Secure ID has been incorporated into the sign on procedures.

Administrative Department:

There are four major departments in GIAC/ME, each with their own special needs and each with functions that are shared. The Administrative Department meets those needs by providing for central billing, central appointment scheduling, payroll, IT service, and general office administration. The servers that provide these services are located behind a firewall outside of the DMZ. These systems are important to the operations of GIAC/ME, each department relies on the data being current and correct. These systems are back-up nightly to tape and those tapes are stored at an off-site location.

The Administrative department handles all of the appointment scheduling for the medical services that are provided by GIAC/ME along with a central supply ordering system in that the other departments use. By centralizing these services GIAC/ME is able to pass the savings on to the patients.

Medical Departments:

The remaining four departments consist of the Pediatric Center, Adult Services, the Free Clinic and the Pharmacy. These departments share the Patient database, Insurance database, and nursing services. With the four departments sharing the information it is imperative that the data is kept confidential, and that the integrity and availably of the patient data is not compromised. The use of the single sign-on and role based access insures that the data is seen only by those who have been authorized. There are redundant servers in-house in the event that a server should have a problem. The databases are saved to tape each night and the tapes are stored in an off-site location.

The patient database currently resides on a Windows server in the offices of GIAC/ME. While in the office, staff members have access through the office intranet. A Check Point firewall sits in-between the switch and the server farm. The firewall allows the internal LANs to pass through to the servers and routes others in to the DMZ. If the medical staff is off-site and requires access to the patient data, they would be directed into the DMZ where the Secure ID server resides and they would be prompted for their pass code and token number.

Assignment Two: Identify Risks

This section is meant to identify the three most critical areas of risk to the organization, one must be a risk to the “crown jewels”, and the other two should be of the top areas of concerns/risk.

GIAC/ME is a small organization and as such it does not have the staffing in the IT section to do most of the housekeeping or security policy needed to keep the environment secure. A formal security policy has not been created, nor has a full security risk assessment been done. Most of the security work that has been done is by the network and database administrators.

Because of the Federal regulations, HIPAA in general, the protection of patient data and the transmission of such data needs to be protected.

The IT section has assigned these duties to an outside contractor and they have discovered the following risk and have suggested remedies.

Areas of Risk 1 – Patient Data Base

Protection of the “crown jewels’ of GIAC/ME is the number one priority for the IT section of GIAC/ME. The crown jewels of GIAC/ME would be the protection of the patient database. GIAC/ME sees many patients per day for any number of reasons. Many of the patients, if not all, would not want their medical record to be the subject of unauthorized access. Neither would the patient want their medical records lost, destroyed or alter in any way. There are also Federal regulations (HIPAA) requiring the protection of this data.

As discussed earlier, the patient database currently resides on a Windows server in the offices of GIAC/ME and is accessed internally thru a firewall and externally through the DMZ where the Secured ID server resides. Medical staff members have a unique sign-on code that allows them to access only the data that they have been authorized to view or update.

While these steps protect access to the patient data there are several items that need to be addressed in order to “tighten up” security.

- Virus protection on each workstation and database server
- Data encryption of patient data across the internet and intranet
- Addition of a Intrusion Detection System (IDS)
- Destruction of paperwork

Virus Protection

Each workstation and server needs to have full time Virus protection installed and updated on regular bases. Virus can have a devastating effect on the computer systems that they attack. Unprotected systems can have their hard drives erased, system files destroyed or any number of harmful processes installed on the organizations computers. Some viruses such as Trojan Horse are used to gather information such as ID and passwords so a hacker can gain access to the system. Computer worms can embed themselves deep into the operating system code only to be released in the future causing havoc to the systems.

Virus can be delivered to the workstation in several different manners. The most poplar is through the email system as an attachment that the user opens. Viruses can be embedded on a floppy or CD that has been infected and will infect any machine that opens the files on the media. By simply surfing the web and going to a web-site that is infected your machine can be infected.

It is strongly recommend that an enterprise wide virus protection be installed on all workstations and servers in the organization such a Symantec AntiVirus Corporate edition.

Data Encryption

Each time a patient record is accessed by a user, the patient data is going across the network in clear text. Anyone that is attached to the network can sniff the line and read the data, causing a compromise of that data. Hackers are always trying to get into data systems to see what they can find. If a hacker were to identify one of the patients in the GIAC/ME that has an aliment such as AIDS, releasing of that information would cause great harm not only to the patient, but also to the organization's reputation. The breach would also allow the organization to be sued for not taking precautions to fully protect the information.

It is strongly recommended that data encryption be installed so that all patient data is encrypted between the workstation and the server.

Intrusion Detection System

As mentioned above, hackers are always looking for systems that they can break into or cause disruptions such as denial of service (DOS). Before a system is attacked there are often things that a hacker will need to do to see if the networked can be broken into. An Intrusion Detection System can allow the administrator to monitor activity of the network and determine if certain items are normal or are the beginning of an attack or break-in.

There are several databases in the GIAC/ME server farm that need special attention. These are the Patient database, Insurance database, and the accounting database. Compromising these servers and the data that resides on

them would cause great embarrassment to both the patient and the organization. Loss of this data could jeopardize patient care, patient confidence in the organization and open up GIAC/ME to law suits for not protecting the patient's information

Destruction of Patient Paperwork

During our risk assessment it has been noted that paperwork such as patient reports, lab request, medical notes and other paperwork were being thrown out with the normal trash. Since this is patient information it must also be protected from unauthorized access. Once an organization throws out its trash, it become available for someone to search through looking for information to use. As stated above the release of this information can cause embarrassment to both the patient and the organization and possibly causing a break in the public's confidence in GIAC/ME.

Shredding of all patient information and any paper that has a patient name on it must be instituted in the organization. It is best to hire a company that will shred the paperwork onsite rather than removing the paper and shedding it back at their offices. http://www.proshred.com/news.html

Area of Risk 2 – Business/Network Recovery Plan

While a major disaster is unlikely, GIAC/ME does not have a plan to recover from a disaster of any size. Whether it's a storm that knocks out the power in the office for days making the office unusable or having a hard drive failure on a critical server, a recovery plan is needed. Having a contingency plan is part of the HIPAA regulations.

In the event of a failure it is critical that there are contingency plans. The ability to treat patients is core to the mission of GIAC/ME. Having access to the patient's medical records is one of the key tools that the medical staff uses. While a paper patient record is available, the ability to have the electronic record enables the medical staff to quickly treat the patient.

The patient record, patient appointments, inventory of medical supplies, accounting and receiving databases are all stored on the computer systems. The inability to access these systems will result in loss of services that are provided to the patients and the inability of the medical staff to effectively treat patients. All this will result in a loss of confidence in the staff.

The IT staff performs backups on all databases in the GIAC/ME server farm and these tapes are stored off-site. However, they do not have the operating

systems, general user files, or the configuration files for the router, switch and firewalls backed up. The loss of these systems and files would make recovery difficult and extend the total amount of downtime.

The router is the only access to the internet and if there was a failure with the router it would prevent access to the internet and the offices web-sites would be unavailable to outside users. Intranet access would not be interrupted since the switch is behind the router allowing the internal LAN addresses through to the servers.

All the hardware that makes up GIAC/ME network has a maintenance contract with a response time of 2 hours by the vendor. This includes the network switches, hubs, servers and workstations that are located in the offices.

It was determined that the acceptable downtime for this is 6 hours. During this time the office would run in a manual mode. Medical staff would use the paper medical record and all the information would have to be entered into the systems once it is back up.

The purchase of redundant servers for backup or the installation of high availability servers could be used to reduce the outage if a failure should occur. It is important that a Business/Network recovery plan be created and implemented. This would give the IT staff a clear directive in what needs to be recovered in order to resume business in the event of a disaster or failure.

Area of Risk 3 - IT Security Plan

GIAC/ME does not have a security plan to set policy in protecting the data stored on their network. Developing a security plan, developing policies with guidelines and procedures is of the up most importance. The proposed HIPAA regulation states that each health care provider has a plan to protect the security of patient data.

By having a security policy the organization is setting up rules of behavior in how they will protect the network and the data that resides on the network. Policies would address the following areas in order to be compliant with the HIPAA regulations:

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security mechanisms

Administrative Procedures

Each organization must have administrative procedures in place to protect the integrity, confidentiality, and availability of patient information. This would include certification of the security of the systems, security training for all staff members that have access to patient information, contingency planning, incident reporting procedures, risk assessment and management and penalties for abuse and misuse of systems.

Physical Safeguards

The physical safeguard of patient information is central to compliance with HIPAA and needs to be addressed in a security policy. Procedures and guidelines would have to be created in the following area:

- Media Control
- Physical Access Control
- Workstation Use/Placement
- Disposal of electronic equipment
- Disaster Recovery
- Security Awareness Training

Technical Security Services

Technical security services are the processes that are put into place to protect and control individual access to information. When developing policies for this area, it is important to include access control, audit controls, authorization controls, data authentication and entity authentication.

Technical Security Mechanisms

How the patient data is accessed is the fourth area of concern for a security policy that will be HIPAA compliant. Communication and Network controls are defined in this area. Whether or not dial in access will be allowed and if allowed, how will the data be protected? Access control and encryption are key areas of concern.

Since the organization is using a network for access, some form of an alarm, audit trail, authentication and event reporting must be defined and implemented. Developing the procedures and guidelines for an IDS and firewall, along with monitoring access to data needs to be created.

Assignment 3 – Evaluate and Develop Security Policy

This assignment is to take a policy and identify its strengths and weaknesses and then to make recommendations to improve and tailor the policy to your site's needs. I have chosen a sample policy from the SANS Security Policy web site @ http://www.sans.org/newlook/resources/policies/policies.htm#template

and used the template Lab_Anti-Virus_Policy which is below –

Lab Anti-Virus Policy

1.0 Purpose
To establish requirements which must be met by all computers connected to <Company Name> lab networks to ensure effective virus detection and prevention.

2.0 Scope
This policy applies to all <Company Name> lab computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

3.0 Policy
All <Company Name> PC-based lab computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into <Company Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Refer to <Company Name>'s *Anti-Virus Recommended Processes* to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are excepted at the current time.

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

5.0 Revision History

Evaluate Security Policy

In reviewing this Anti-Virus Policy I found that it was very readable and when you finished reading the policy you had an understanding of what was expected and what must be done in the event of an infected machine. Overall it is a good basic policy.

What I will attempt to do is to do a critical review of each of the sections included in that policy.

Purpose – A one sentence, brief statement saying that all computers connected to the network will have effective virus protection and detection. This is brief and to the point, no words wasted.

What the purpose doesn't say is why it's important to have this policy. It doesn't say that if a virus infects one computer that it has a chance of infecting other computers on the network. It almost assumes that you know what to expect and why.

Scope- Again, a short brief statement saying that all computers, rather all PC computers or computers that access PC file systems, or generate traffic are covered by this policy.

While is it brief and to the point I would prefer that it add clarity. Saying that PC-based or utilize PC-file directory sharing could be unclear to the normal user. Using the terms "but not limited to" is sort of legalese and could be said in another way to make it more readable. Limiting a virus policy to only PC can cause problems since a Mac can transmit viruses and other Operating Systems have their own problems with viruses.

Policy – This is well written and fully explains what the policy is. It also refers the reader to other policies and guidelines. It explains what the policy is – all PC-based computers must have virus protection and that the virus patterns are kept up-to-date. The policy defines who is responsibility it is to enforce the policy – Admins and Manager are responsible for creating procedures to ensure virus protections is running.

Over all this are very straight forward and a direct policy statement.

Enforcement – again, a one sentence statement that clearly states that any employee found without protection may be subject to disciplinary action including termination.

While this statement and the overall policy are clear, and the policy is well written – I do not feel that it is enforceable in its current configuration. If the user has brought you on disciplinary action they could have an out by stating that they really didn't understand the importance of the policy. The reader of this policy is told that they must have virus protection on their machines, that it is up to management to ensure that virus protection is running and that it is current. There are, in somewhat hazy terms, the What, How, Who, but they are not told the Why. In my opinion this is one of the most important aspects in writing a policy – to let the reader know "why" the organization is putting forth a policy.

Revise Security Policy

It is my attempt to revise and write this policy to improve its readability and to add to it the why. I will attempt to incorporate the comments I have made above into this new policy.

GIAC/ME Anti-Virus Policy

1.0 Purpose

The purpose of this policy to ensure that all computers (Workstations and Servers) that are attached to GIAC/ME's network have continuously running virus protection installed and operating. Viruses, Trojan horses, and malicious software can infect any machine that is not properly protected. These viruses can cause permanent lost and/or corruption of the data that resides on our workstations and servers.

2.0 Scope

This policy applies to all computers and computer systems that are attached to GIAC/MEs network and to computers and computer systems that are owned by GIAC/ME.

3.0 Policy

All GIAC/ME computers must have installed and operating anti-virus software that is approved by GIAC/ME. This software is to be continuously running and must be set up to receive regular nightly updates to the virus definition patterns and anti-virus software updates. In addition, each computer must be checked nightly to ensure that it is virus free.

A virus infected computer must be reported to the ISSO and those computers will be removed from the network until they are certified to be virus free.

Any activities with the intention to create and/or distribute malicious programs into GIAC/ME network are prohibited, in accordance with the Acceptable Use Policy.

GIAC/ME managers and supervisors have the responsibility of ensuring that all computers in their area comply with this policy. To assist managers, supervisors,

and users please refer to GIAC/ME guidelines on Anti-Virus Recommended Process to assist in preventing infestation of computer related viruses.

All employees of GIAC/ME will be required to read this policy and sign that they understand it and agree to follow its directions.

4.0 Enforcement

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

Assignment 4 – Develop Security Procedure

It will now be my attempt to develop a "Security Procedure" for the Anti-Virus Policy

Guidelines for installation of Anti-Virus Protection

Background

Here at GIAC/ME it is the official policy that all computer workstations, laptops, and system servers have installed and running anti-virus protections. GIAC/ME has a site-license with Network Associates' McAfee VirusScan. The software can be downloaded from the Anti-virus server. Please see http://www.nai.com for a description of McAfee Virus Scan software.

Protecting the information stored on all the systems and servers within GIAC/ME is a priority and critical to our organization. HIPAA regulations state that the confidentiality, integrity, and availability of patient data be protected. Should one of our workstations or severs become infected with a computer virus that computer could destroy or compromise the patient data, could allow a hacker to gain access to our network and even shut it down, steal the data, or even change the data on the system.

Ensuring that each machine's virus protection is up-to-date and continually running will help prevent our systems from being infected.

Installation of the Anti-Virus software and setting up the software will be the responsibility of the system administrator for each department. It will also be the responsibility of the system administrator to check that the virus protection software is operating correctly on a monthly basis.

Procedure:

To install the McAfee VirusScan the following steps need to be completed

- Go to the GIAC/ME security web-site and down load the Anti-Virus software @ www.giacme.org - find the correct client for your machine
- When prompted to either Open or Save the file select Save and Save to a folder called Virus Protection
- When the download is complete, open the folder and double click the file, this will unzip McAfee software - please to unzip into the same folder when prompted
- Once it has finished, select the VirusScan Setup to install
- Follow the instruction for installation:
  - Select Use Maximum Security
  - Select Typical Installation
  - Select Install
  - Deselect the Run default Scan after Installation
  - Select AutoUpdate Now
- Once the AutoUpdate has completed you are finished with the Installation

After the software has been updated it is available and now you must update the configuration.
To update these files you must start the VirusScan Console. This can be done by either double click on the "magnifying glass icon on the toolbar or select the program from the program list – Network Associates and select the VirusScan Console.

First update the AutoUpdate

- Select the AutoUpdate
- Select Configure
- Select Edit (their should be a update site selected)
- Confirm that the site says Network Associates
  - The Retrieve File From is FTP
  - The FTP Site is – ftp.your.ftp.com/virusdef.4.x
  - Select Next twice – this brings you back to the properties
- Select Schedule
- Select Enable and Daily
- Select enable randomization at 01:00
- Apply these changes
- Select Program and Run Now

Second update the AutoUpgrade

- Select the AutoUpgrade
- Select Configure
- Select Edit (their should be a update site selected)
  - If no site, Select Add
- Confirm that the Site says Network Associates
  - The Retrieve File From is FTP
  - The FTP Site is – ftp.your.ftp.com/upgrade.xx
  - Select Next twice – this brings you back to the properties
- Select Schedule
- Select Enable and Weekly
- Select enable randomization at 01:00
- Apply these changes
- Select Program and Run Now

Third Schedule daily running of the Virus protection

- Select Scan My Computer
- Select Schedule
- Enable to run daily at 23:00
- Apply these changes
- Select Program and Run now to check

As stated above each System Administrator will need to check each machine at least monthly to verify that the VirusScan has indeed run and to check to see if there were any errors.

To verify that the VirusScan has been running either double click on the "magnifying glass icon on the toolbar or select the program from the program list – Network Associates and select the VirusScan Console.

Confirm that the AutoUpgrade, AutoUpdate and Scan My Computer have run successfully and that there is a date and time in the Next time column. If there have been errors please refer to guidelines on Error Checking of Virus Scanning Software.

Reference:

Cisco Information

http://www.cisco.com/univercd/cc/td/doc/pcat/1760.htm#CIHFBEEI –

http://www.cisco.com/univercd/cc/td/doc/pcat/ca2926.htm

http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/

http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm

RSA SecurID

http://www.winnetmag.com/Articles/Index.cfm?ArticleID=26315&pg=4
http://www.rsasecurity.com/products/securid/index.html

Virus Information

Symantic - Symantec Enterprise Security Manager™ for HIPAA 1.0 –
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=162

Network Associates – McAfee VirusScan
http://www.nai.com

HIPAA –

Alexander J. Brittin, Dana B. Pashkoff, and John P. Tedesco, The HIPAA Handbook: What Your Organization Should Know About the Proposed Federal Security Standards.
URAC American Accreditation Healthcare Commission ISBN 1-930104-08-1

Centers for Medicare & Medicaid Services – DHHS
http://cms.hhs.gov/hipaa

SANS – What's all the hype on HIPAA
http://www.sans.org/newlook/resources/policies/policies.htm#HIPAA

Security Shredding Services

http://www.proshred.com/news.html