Global Information Assurance Certification Paper

CASE STUDY: MANAGING AN INFORMATION SECURITY PROGRAM IN THE HEALTHCARE INDUSTRY

Dave Jahne, CISSP
GSEC Version 1.4
June 21, 2002

Introduction

The disciplines of information security have been in practice for several decades. Industries such as manufacturing, government, and finance have long realized the necessity that protecting their company information is a critical component of doing business. However, the healthcare industry has not always been as proactive as other industries in addressing information security. In fact, the federal government passed a law in 1996 (The Health Information Portability and Accountability Act, known as HIPAA) that establishes a set of security regulations that covered healthcare entities are mandated to comply with.

The objective of this discourse is to provide the reader with an insight as to one organization's approach with instituting a formal information security program. The paper will briefly discuss the HIPAA security regulations, as they are the primary driver of the healthcare industry's information security initiatives. The paper will then present an overview of the information security office's strategic and tactical plans; share the challenges, experiences, and solutions encountered; and thoughts on the correlation of patient privacy and information security within the mission of providing patient care.

For reference purposes, the case study organization is a healthcare provider with facilities in several states. The organization has multiple data centers providing information services to the facilities and the 20,000 employees.

Background

"The healthcare industry has built information systems without the sufficient granularity required to adequately protect the information for which we are custodians. Many of the existing systems require no more than a three-character log-on ID; some have passwords that are shared by all users; and most have not implemented the appropriate classification of access controls for the jobs that users perform." [1]

Lack of security policies and standards, un-audited access control lists, and poor Web site configurations are some other examples where healthcare organizations demonstrate a failure to follow basic security controls and practices.

One of the objectives of HIPAA is to protect the confidentiality and integrity of patient health information. Attaining this objective requires that security around the information be sufficient to protect the information from accidental or intentional disclosure, plus assuring the accessibility of information. To this end, the Department of Health and Human Services (DHHS)

is overseeing the establishment of the HIPAA security regulations. The regulations are intended to "provide a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual... The Security standard mandates safeguards for physical storage and maintenance, transmission, and access to individual health information. It applies not only to the transactions adopted under HIPAA, but to all individual health information that is maintained or transmitted." [2]

HIPAA Security Regulations

Following is a brief overview of the security regulations to assist the reader in understanding the 'why' behind the development of the organization's strategic and tactical plans.

The security regulations are designed to be 'technology-neutral' so that healthcare organizations can secure information according to their circumstances. Furthermore, the regulations are intended to set a minimum level of security and organizations may choose to implement stronger safeguards than mandated.

Under HIPAA healthcare organizations are required to:

- "Assess potential risks and vulnerabilities.
- Protect against threats to information security or integrity, and against unauthorized use or disclosure.
- Implement and maintain security measures that are appropriate to their needs, capabilities and circumstances.
- Ensure compliance with these safeguards by all staff." [3]

HIPAA refers to affected healthcare organizations as 'covered entities'. Covered entities are health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form. The regulations are grouped into three discrete arenas that are intended to provide a comprehensive umbrella towards protecting data confidentiality, integrity, and availability.

The first arena is Administrative Procedures, which consists of twelve areas of documented, formal practices to manage the selection and execution of security measures. The twelve areas are:

1. **Certification** –Certification is the process of determining whether technical security controls are implemented and comply with specified criteria. Each covered entity is required to establish a certification process that demonstrates and documents that its computer systems and networks meet these criteria. Either internal staff or external persons may perform certifications. The process should consider risks identified in the risk assessment process.
2. **Chain of Trust Partner Agreements** –A Chain of Trust Agreement is required between two business partners whenever data is electronically exchanged. The Agreement requires that the sender and the receiver of the protected health information work with each other to maintain the

information's integrity and confidentiality. Such contracts provide a legal basis for maintaining consistent levels of data integrity and confidentiality.

3. **Contingency Plan** – "Each covered entity is required to maintain a contingency plan for responding to system emergencies involving systems that contain protected health information. The covered entity is required to perform periodic backups of data, have critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place for such systems.
4. **Formal Mechanism for Processing Records** – Covered entities are required to maintain documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of protected health information.
5. **Information Access Control** – Each covered entity is required to establish and maintain formal, documented policies and procedures for granting different levels of access to protected health information. These policies and procedures must, at a minimum, include:
    - Access authorization policies and procedures.
    - Access establishment policies and procedures.
    - Access modification policies and procedures.
6. **Internal Audit** – This requirement calls for periodic reviews of a covered entity's internal security controls, including records of logins, file accesses, and security incidents.
7. **Personnel Security** –Each covered entity must establish a personnel security clearance process to administratively determine that persons and computers are trustworthy before giving them access to protected health information. This process must account for, and document, levels of access granted to individuals, programs, and procedures. The process must also address persons who fill roles where incidental access to protected health information may occur, such as system and network support and maintenance personnel. Supervision of un-cleared or unauthorized personnel, such as support and maintenance personnel, is necessary unless their access to protected health information can be precluded.
8. **Security Configuration Management** – A covered entity is required to have written security plans and procedures guiding its security efforts so as to create a comprehensive security program. The security program must include an inventory of system assets, formal procedures for installing and testing new systems, a regular security testing

schedule, and virus checking.

9. **Security Incident Procedures** – The covered entity must have written procedures for reporting security breaches to ensure that security violations are handled promptly and appropriately. These must include:
    - Procedures for reporting security incidents.
    - Procedures describing response, i.e. actions to take when a security incident is reported.
10. **Security Management Process** – An overall information security management process is necessary to establish policy, provide oversight, and administer operational aspects of the program. Supporting policy statements and procedures are required to facilitate the prevention, detection, containment, and correction of security breaches. Specific areas that the security management process must cover are: risk analysis process, risk management process, sanction process, and security policy.
11. **Termination Procedures** – Entities must revoke physical access to controlled areas and remove user accounts when an employee's employment is terminated or when others, such as contractors and vendors, no longer require access. Although this point is entitled "termination," the text includes provisions for other occasions in which removal of access rights is called for.
12. **Training** – Security training is necessary for all workforce members who access protected health information. This training must include overall security awareness, periodic reminders, virus awareness, password management, and user-specific topics necessary for individual workstation security. [4]

The second arena is Physical Safeguards, which consists of five areas geared toward the protection of computer systems and related buildings and equipment from hazards and intrusion. The five areas are:

1. **Assigned Security Responsibility** –The governing body of each covered entity must designate a security officer or group to oversee the safeguarding of protected health information and assign the necessary responsibility and accountability to that role. This person or group will manage the execution and use of security measures and supervise the conduct of personnel in relation to data protection.
2. **Media Controls** –While this item states that it is focused upon the transfer of hardware and software media into and out of a facility, it also requires consideration of the larger issue of how to handle record copies of protected media from creation to destruction. Each entity will need to decide how to categorize, annotate, account for, store, and dispose of protected health information in record form.

3. **Physical Access Controls** –Each covered entity is required to establish formal, documented policies and procedures for limiting physical access while ensuring that properly authorized access is allowed. Mandatory implementation features also include plans for emergency operation and disaster recovery as well as for testing and revision.
4. **Work Station Use** – Each covered entity is required to establish a policy/guideline on secure workstation use. These documents will establish the rules for minimizing the risk of exposing protected health information to unauthorized access. They will include technical measures (automatic logoff) as well as behavioral rules (no sharing of passwords).
5. **Security Awareness Training** – Covered entities are required to establish security awareness training programs customized to individual job responsibilities. Training for all workforce members in the use of protected health information and its confidentiality and security is required. [5]

The third arena is Technical Security Services, which consist of six areas of processes that protect and monitor information access. The six areas are:

1. **Access Control** –Each covered entity is required to maintain a mechanism for access control that restricts access to resources and allows access only by privileged entities, providing access only to those workforce members with a business need for it. Possible types of access control include mandatory access control, discretionary access control, time-of-day, classification, and subject to object separation. In addition, a mechanism to enable emergency access is required.
2. **Audit Controls** –System activity logging is required in order to recreate pertinent system events and actions taken by system users and administrators. An audit process of examining logged information is required in order to identify questionable data access activities, investigate breaches, respond to potential weaknesses, and assess the security program.
3. **Authorization Control** – Covered entities must implement a mechanism to authorize the privileged use of protected health information available via systems and applications. The mechanism must limit these privileges to the maximum practical extent commensurate with professional needs.
4. **Data Authentication** – Each covered entity must be able to provide corroboration that protected health information in its possession has not been altered or destroyed in an unauthorized manner. Data corroboration methods include, but are not limited to, the use of checksums, double keying, message authentication codes, and digital signatures.

5. **Entity Authentication** – Entities (an entity may be a person, system, or process) must be authenticated prior to accessing protected health information. Authentication is the process of corroborating that an entity is who or what it claims to be; it may occur through a trusted process such as the provision of a secret password, a personal identification number, or a token. Automatic log offs, or inactivity time-outs, can help enforce authentication by precluding others from accessing unattended sessions.
6. **Communication/Network Controls** – Covered entities that use external communication systems, such as the public switched telephone system, or open networks, such as the Internet, are required to safeguard protected health information that traverses them. The specified technical security services address network risks of message interception and interpretation by parties other than the intended recipient. Additionally, these services protect information systems from intruders attempting to exploit external communication points such as Internet host systems and telephone switches. In addition to the other listed precautions, some form of encryption is required when using open networks.[6]

Overview – Phase I

In the 4th quarter of 2000 the organization established the high level strategies defining how information security would be addressed. In the short-term, the strategy is to interpret the HIPAA security regulations within context of the organization, conduct a gap analysis of existing privacy and security practices measured against the regulations, and prioritize the HIPAA remediation projects. In the long-term, the strategy is to build the information security office so that information practices will be sustained beyond the HIPAA compliance date.

Based on the strategy, it was determined that the initial steps entailed:

- Assigning security responsibility to an office (Information Security Office) that is dedicated to and accountable for information security.
- Conducting the HIPAA gap analysis (Risk Assessment) across the organization so that privacy and security practices are measured in all facilities.

The Information Security Office (ISO) is now the initiator and facilitator for the organizations' strategic and tactical security planning.

The core group within ISO consists of three full time employees; the ISO will report to the Chief Information Officer once the HIPAA compliance is attained. A security advisory group consisting of senior management from the Information Technology, Risk Management, Safety and Security, Human Resources, and Legal departments has been formulated to assist the ISO in

identifying and prioritizing security initiatives. There are also 'points of contact' at the facilities and data centers to serve as liaisons for security-related issues.

The primary challenge in this concept is to guard against 'security by committee', which could lead to a paralysis of initiatives. This, fortunately, has not yet happened but is certainly something to remain vigilant against.

The HIPAA gap analysis was conducted in 2001. The objective of the analysis was to survey each facility to understand the facilities' existing privacy and security practices, and then develop remediation plans based on the analysis.

To facilitate conducting the survey, the ISO purchased an automated risk assessment tool. The software proved useful for distributing and collecting questionnaires; however, some tweaking of the product was necessary to fully meet the needs of the organization. The software has been marketed as a security risk assessment tool and the vendor essentially retrofitted the tool to become a HIPAA gap analysis product.

The privacy and security officers felt the software did not adequately map the survey questions to the HIPAA regulations, consequently a re-write of the question sets was undertaken. It required approximately four 'man-weeks' from both the senior privacy and security officers to re-write the question sets and bring them to an acceptable level.

Other major drawbacks with the tool were a poor reporting mechanism and unreliable connections with the ASP server. The 'out-of-the-box' reporting function was a template slanted to delivering executive style threat and vulnerability charts. The ISO needed reports that were meaningful to the facilities by demonstrating the gaps uncovered by the survey. To put together meaningful reports, the ISO scripted custom reporting code that was run against ODBC files populated by survey responses. Unreliable server connectivity was an ongoing issue for the length of the survey. This led to degrees of frustration on the user end, ultimately resulting in the survey sample size being decreased.

Despite the drawbacks, the software was determined to be a worthwhile investment simply from making the survey questionnaire distribution, collection, and analysis faster.

The HIPAA gap analysis provided meaningful data from the facilities and has enabled the ISO to determine remediation priorities and budgeting. Other positive outcomes are 1) the ISO now has a benchmark measurement for determining the status of HIPAA compliance in forthcoming years, and 2) distributing the final reports in a presentation meeting environment provided the opportunity to educate and train facilities on the HIPAA initiatives.

Overview – Phase II

Using the information from the gap analysis and factoring budget requirements and resource availability, the ISO began prioritizing security remediation projects. These are tactical projects moving the organization not only toward HIPAA compliance, but also instituting security measures of prevention detection and response. Following are descriptions of the projects. Hopefully these case studies will be of value to other practitioners as they address implementing information security programs in the healthcare arena.

Case Study: Cryptography

Cryptography is an important part in designing a 'defense in depth' security strategy by providing assurances for data integrity and confidentiality. Also, the HIPAA regulations state that some form of encryption is required when transmitting protected health information across an open network.

The approach of the ISO is to implement cryptography solutions into the areas of data file transmissions, e-mail, and portable computing devices. This approach will address HIPAA regulations, provide for the encryption of sensitive, non-PHI data transmitted over the Internet, and also secure data that is subject to compromise by loss or theft.

For transmitting data files, each data center is setting up an FTP server that will encrypt files prior to transmission. The organization has procured Network Associates e-Business server as the encryption mechanism. Policy states that all files containing data that is classified as patient or business confidential data must encrypted prior to transmission over the Internet using the designated FTP server. The largest challenge to date has been identifying the flow of data that originates outside of the data centers.

E-mail encryption is currently in the evaluation stage. It has been determined that encryption has to occur at the mail gateway rather than the desktop. Several products have been looked at and the two being evaluated are Tumbleweed and Clearswift. It appears that e-mail encryption will be costly to purchase (200 – 300K), require additional hardware, and also have a significant administrative commitment. Addressing e-mail encryption will be a complex effort and healthcare organizations will be well served to begin looking at solutions.

The portable computing devices being secured are laptops and Personal Digital Assistants (PDA's). The organization is evaluating a product from Credant Technologies that encrypts folders on PDA's. Mobile Guardian allows for centralized administration of securing PDA's by pushing encryption policies onto the device when it is connected to the network. Utilizing domain groups, only users identified as requiring encryption will receive the encryption policies on their PDA's.

As for laptops, they are in the process of being refreshed from Windows 2000 to XP. Organizational policy will state that laptops containing patient or business confidential data must use Microsoft's EFS application for encryption. Issues around using EFS are user education, key management, and a method of verifying that EFS is being used. Although depending on the end user is not optimal in the security world, in the healthcare industry funding is not always readily available and many times the ISO must be creative in implementing solutions.

Case Study: Policies & Procedures

The cornerstones of an information security program are clearly defined and communicated policies. The ISO has written a comprehensive security policy that is in the final approval stage. The policy speaks to individual and departmental accountability and authority;

access control; administrative passwords; audit & logging; encryption; Internet and e-mail usage; remote access; information disposal; information recovery; physical and environmental security; security awareness training; violations & sanctions; unauthorized software; and virus protection. A lesson to be imparted is to begin work immediately on policies as the approval process can be lengthy. It has been my experience that the larger the organization, the longer the approval process.

The gap analysis revealed that facilities and data centers were lacking procedures to notify security administrators in a timely fashion when accounts need to be removed from computer systems. To resolve this, the ISO initiated a project in conjunction with Human Resources. The objective of the project was to design a procedural method whereby HR and security administrators would be notified promptly of an employee's termination. An Intranet form was designed that is used by managers when an employee is terminated. When submitted, HR personnel and security administrators are e-mailed of the pending termination date and the employee's account is flagged for de-activation. In addition to resolving a security gap, the project has also been beneficial in that ISO and HR seized the opportunity to work in a co-operative setting, thus building teamwork and respect between the departments. As the information security program matures, it is paramount that such relationships are continually developed and nourished.

Good security depends upon prevention to, detection of, and reaction to security incidents. Computer Incident Response Teams (CIRT's) are being put in place in the organizations' data centers and will eventually encompass the facilities. CIRT's have currently been built for two network service departments and one telcom department. The same standard is used for each team, that being the CIRT's are based on the SANS six steps of Incident Handling – preparation, identification, containment, eradication, recovery, and lessons learned. [7]
As with other areas of the information security program, support from the executive level was very helpful in getting departmental buy-in to the CIRT concept.

Case Study: Awareness & Training

All users must be made aware of good computing practices and educated about computer security. This is one of the most important aspects of a secure environment because users must understand the environment they work in and their responsibilities inherent within their environment.
Developing an effective awareness & training program is no small task. The audiences need to be identified and targeted. For example, I/T staff will receive a different type/level of training than the clinical staff. There is also the challenge of reiterating basic content in a new and refreshing manner.
The ISO is developing the security awareness & training program as a

phased project. The communication vehicles decided upon are 1) an internal ISO web site, 2) utilizing the company newsletter, 3) formal periodic presentations, 4) a poster program, and 5) computer based training (CBT).
In line with the phased project approach a three-year deployment plan is being put together. Each year a deadline schedule is set up for submissions to the company newsletter. Also, at the beginning of the year, quarterly presentations are scheduled for facility departments. The poster and CBT programs are budgeted annually and new products purchased as needed. The security web site is under design and is being developed as both an informative site and a place for employees to submit security related questions and concerns.
The ISO, despite being slightly over a year old, has already conducted over 20 presentations for various departments. These 'face-to-face' engagements are proving very effective for educating employees on both information security expectations and the upcoming HIPAA regulations.

Case Study: Intrusion Detection System (IDS)

The organization's data centers incorporate firewalls as part of the perimeter defense strategy. However, because none of the data centers has implemented an IDS, installing and configuring IDS's for the data centers is a current ISO project.

There are two primary types of IDS's – Network IDS (NIDS) and host based IDS (HIDS). NIDS's use sensors placed on the network to monitor traffic and determine if there is unusual activity. HIDS's are designed to detect suspicious activity or known attack patterns on the specific host the sensor is installed on. Proper deployment of an IDS should include using both types.
The ISO is deploying SNORT for the internal NIDS, Cisco's NetRanger for the external NIDS and will purchase Tripwire for the HIDS. The ISO is now in the IDS policy development stage.
Deploying the IDS is requires careful and thorough planning. Once the hardware/software is decided upon, an IDS policy needs to be drafted that will serve as a guide for the implementation process. Some issues that should be addressed in the policy are restrictions on network traffic, who will be authorized to change IDS policy and/or configurations, on which machines and wires will sensors be installed, and determining who is responsible for monitoring and responding to alerts. It's anticipated that the entire project will take about a year to complete.

Case Study: Vulnerability Assessment

Because a security vulnerability assessment has never been done for the organization's network environment, ISO sponsored the procurement and scheduling of such an assessment. It was determined that more value would be realized by having the assessment conducted by a third party. The assessment's goals are 1) identify network security vulnerabilities using proven vulnerability assessment and penetration

testing methodologies and, 2) provide the organization with a baseline measurement of its security posture and infrastructure. For clarification purposes, a vulnerability assessment is a comprehensive look at systems, policies, procedures and the network whereas a penetration test is a snapshot in time of a network's vulnerabilities.
The assessment's scope includes modem war dialing; host assessments of UNIX, Novell, and Window servers; server policy and procedure analysis; Internet server penetration testing; Internet infrastructure policy and procedure analysis; network device (router & switches) analysis; VPN assessment; and firewall penetration testing.
Future assessments will include such items as wireless analysis, IDS assessment, and AS400 & OS390 assessments.
The processes for initiating the assessment were made easier by having executive support and budget approval. The upcoming challenge for ISO will be the project development and leadership responsibilities for seeing the remediation tasks to completion.

Case Study: Upcoming Initiatives

Two projects that are just beginning are the disaster recovery/business continuity plan (DR/BC) development project and the desktop security project.
The approach for DR/BC is to contract a consulting firm to write the plans. The chosen vendor will be expected to lead the planning committee, conduct the business impact analysis, establish the priorities for processing and operations, determine recovery strategies, perform data collection, organize and document the written plan, develop testing criteria and procedures, and testing the plan.
The desktop security project is heavily entwined with HIPAA privacy issues and focused on the facilities. Potential solutions will be privacy covers for monitors in areas that are accessible by persons unauthorized to view patient data, automatic logoff mechanisms, forcing unique id's, and enabling access controls that restrict access to resources by allowing access to privileged, approved entities.

Using the HIPAA gap analysis and the vulnerability assessment report, the ISO will be formulating the security budget and initiatives for the coming year. A major project will be developing centralized management of logging and auditing. This will entail identifying critical data flows and the correlating platforms to that should be logged; placing the logging information on a dedicated server; automating a process to combine files and flag anomalous behavior; and design an alerting and response methodology.
For additional assurance, the ISO will be designing and implementing a mechanism for scheduled automated vulnerability scanning. There will also be a schedule of security reviews for applications and operating systems.
Developing security policies and procedures will constitute a large part of the ISO's activities. They will be in such areas such as media control, security certification and testing, access control matrices, personnel

security clearance, computer asset inventorying, security breach handling, physical access controls, work station use, and audit requirements.

Correlating Patient Privacy & Information Security

Protecting patient privacy is a fundamental business decision for healthcare organizations. One of the ways this business decision is supported is by instituting an information security program. An organization can have security without privacy, but cannot have privacy without security.

The privacy office and security office must work closely together to protect patient information. In the organization, policies developed by the privacy office are reviewed by the security office and vice versa. Control areas such as data classification and access matrices are jointly developed. HIPAA education sessions have representatives from both offices to reinforce the meshing of privacy and security. A facility walk-thru is also jointly conducted to make sure findings reflect privacy and security.

Here are five basic concepts to consider within the healthcare industry, 1) patient information must move in non-secure spaces, such as the Internet, 2) that information must be secured, 3) the security solutions must be integrated with existing systems, 4) the solutions must be reasonably easy to implement, use and maintain, and 5) the solutions cannot be cost prohibitive.

At the end of the day, organizations are in the business of providing healthcare, not complying with government regulations. This is not say that the HIPAA regulations are insignificant or can be ignored, rather that practicing due diligence with a healthy dose of common sense is the key to successful management of a healthcare information security program.

Endnotes: