Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Shift to Security Implementation in a HealthCare facility

There are a number of challenges presented to healthcare facilities as they begin the shift to implementing Information Security. One of these is that they have often been among the first to adopt new technologies. With new technologies there are always unknown issues that present themselves over time. If not addressed, these can often result in nullifying any advantage gained from early adoption. One such liability with Information Technology is a sometimes-inherent insecurity. As an early adopter of new information t...

Copyright SANS Institute

Author Retains Full Rights

AD

The Shift to Security Implementation in a HealthCare facility

GIAC Security Essentials Certification (GSEC) Practical Assignment (V1.4b)
Option 1

Sean E. Mulch
March 15, 2004

Introduction

The healthcare industry has always been an early adopter of new technologies. The emergence of Information Technologies in recent decades has provided the industry with new tools to provide better patient care. Since quality of care has always been the technology driver in the healthcare industry, Information Security has often been given little, if any, consideration.

Recent government mandates have made security a stated priority in the healthcare industry. However, the unique environment of a healthcare facility can pose very real challenges to implementing Information Security. Many healthcare facilities now find themselves in an almost paradoxical predicament: inherently insecure and complex systems are required to be supported to maintain quality of healthcare, while security by mandate must be implemented and insured. As of the writing of this paper, many facilities have likely begun addressing specific security issues. However, these are often being done in a project-oriented fashion with a defined goal of achieving current compliance with regulations. This paper addresses methods that can be used to approach and address security in a dynamic fashion specifically tailored to the needs of larger healthcare facilities, recognizing security as a discipline rather than a destination. It has been written with the approach of both guiding initial implementation and providing a resource for periodic re-evaluation of current implementations.

The Challenges

There are a number of challenges presented to healthcare facilities as they begin the shift to implementing Information Security.

One of these is that they have often been among the first to adopt new technologies. With new technologies there are always unknown issues that present themselves over time. If not addressed, these can often result in nullifying any advantage gained from early adoption. One such liability with Information Technology is a sometimes-inherent insecurity. As an early adopter of new information technologies and systems, a healthcare facility will often find itself assuming inherent security vulnerabilities, which are either not yet known or not yet addressed by industry.

Another challenge is that many healthcare Information Technology vendors build systems focusing on health services with little, if any, consideration to security risks. While new government mandates are affecting a shift in this approach, there are still many systems in place that were designed and installed without thought of security. This issue is compounded by the fact that many purchase decisions are made by those who, while understanding the healthcare provided, do not understand the underlying technologies and security issues presented by their implementation.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

When multiple health services are offered in a facility, there can often be a large number of disparate systems being implemented. This becomes a challenge to maintain Information Technology standards as well as support. Additionally, when interoperability is required between such systems, it can be challenging to do so in a secure manner. With many systems being used simultaneously, it can be difficult to keep a grasp on all the needs and issues presented by each system. This makes security difficult, as there is often pressure to quickly implement and maintain the systems, thus relegating security to an afterthought.

Once systems are implemented they quickly become heavily interdependent and relied upon by staff. Thus upgrades, patches, and other security efforts must be carefully choreographed. In addition, there is often a culture of 'status quo' within a healthcare facility. Therefore, cooperation in addressing security issues in one or more systems can be hard to attain.

Finally, since healthcare facilities have many publicly accessible areas there is a great need for physical security. Healthcare facilities are increasingly concerned with providing resources to patients and family to improve their overall comfort. Many of these resources are computer based and can pose further risks to the overall security of the facility. So the challenge is to provide the patients with these resources while still protecting critical systems.

The Advantages

While the challenges presented by the uniqueness of the healthcare industry can be formidable, these can also present certain advantages.

A major advantage is the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Within the industry this act has received a large amount of attention. HIPAA presents requirements that the industry insure the privacy of protected health information (PHI). Given the recognized uniqueness of the healthcare industry, the draft Security Policy stated:

> There is no recognized single standard that integrates all the components of security …that must be in place to preserve health information confidentiality and privacy as defined in the law. Therefore, we are designating a new, comprehensive standard, which defines the security requirements to be fulfilled.[1]

These newly defined security requirements can be used as a catalyst within a facility to implement comprehensive security measures.

Another advantage is that recent events have brought increased security awareness to the population at large. World events have drawn attention to the need for physical security. A culture that is increasingly litigious regarding privacy rights has raised awareness of the liabilities associated with failure to implement both

---

[1] U.S. Department of Health and Human Services. "Security and Electronic Signature Standards; Proposed Rule." Page 43249 Section D.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

physical and information security. These factors have created a shift in the public culture toward being more cooperative with efforts to implement security.

Additionally, healthcare facilities are often round-the-clock operations requiring a high level of availability from Information Technology systems. This requirement makes protection of these systems of paramount importance. There have been seemingly regular occurrences of highly publicized viruses, worms, and distributed denial of service attacks on information systems that have crippled many organizations. These have raised awareness of the need to provide information security in order maintain systems availability.

Finally, the relative stability of budgets within such facilities is another advantage. As healthcare facilities are often not as susceptible to the overall economic fluctuations, departmental budgets are generally stable. Where other industries may be required to make large budgetary adjustments due to overall company performance, healthcare facilities are not often subject to such factors.

Addressing the Challenge

Due to HIPAA, the primary drive toward security in a healthcare facility will almost certainly be privacy. HIPAA dictates that there must be an Information Privacy Officer (IPO) charged with enforcing HIPAA guidelines. The role of Privacy Officer is defined as specifically pertaining to PHI and generally covers this information in all its various forms. As has been noted by many professionals in Information Security, there is an undeniable relationship between privacy and security. Therefore security will be addressed as a means of protecting PHI. From this starting point, comprehensive security measures can begin to be implemented.

The Information Security Officer

Since privacy and security are so closely related, HIPAA also defines rules for information security and directs that there be an individual charged with enforcing these security requirements. Given the specific knowledge required by this person and the scope of responsibility given this role, it should be filled by a dedicated Information Security Officer (ISO). An ISO role should be created to “Implement policies and procedures to prevent, detect, contain, and correct security violations.”[1] Before designating the person to fill this role, the responsibilities associated with it must be clearly defined and documented. The ISO will need to work closely with the IPO in order to accomplish their common goal.

In the corporate organization chart the ISO should be placed at a level that gives the individual an authority to recommend, implement and enforce policy. The ideal position for the ISO would be directly reporting to the Chief Operating Officer (COO). This would give the position the required authority and avoid any conflicts that may arise from being subordinate to the Chief Information Officer (CIO).

As was stated, the major functions of the position must be carefully defined and documented. Care must be taken not to confuse or overlap the definitions of this role with those of the IPO. Some examples are:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Develop, and maintain reasonable and effective policies and standards designed to maintain the security of all business-related information.
- Insure compliance with all applicable government and corporate mandates as they pertain to information security.
- Perform regular audits of all systems to insure security and identify areas for improvement.
- Provide Information Security consultation to departments.
- Coordinate the evaluation, design, and implementation of systems for protecting and monitoring the integrity of business data and systems.
- Develop, and direct regular security-training initiatives for all employees.
- Coordinate efforts to respond to and resolve security incidents.
- Coordinate a disaster recovery plan that encompasses all critical systems.

The individual chosen to fill this position should be given careful consideration. In addition to the technical skills required, the individual's temperament should be given attention. The dynamic of the general culture in larger healthcare facilities can present a challenge to accomplishing the tasks outlined above. The person undertaking this must have an ability to balance security requirements with usability and user comfort needs. While this is true of any ISO in any industry, healthcare personnel can occasionally present a self-defined authority to dictate or usurp policy. The ISO should have the ability to address challenges to policies in a thoughtful, pragmatic fashion, while avoiding serious security compromises and attempting to promote a cooperative spirit.

A Team Effort

As digital systems continue to expand into every aspect of an organization, the security of these systems cannot be practically addressed by a single individual or even a single department. Simply addressing security concerns within the Information Technology Department may be beneficial. By itself, however, the department will never be able to address all the issues present. Operating independently to address security may result in a constant struggle in which progress is slow and difficult to achieve. Given the breadth of the challenge that security presents to a healthcare facility any approach must also be broad.

In the article *Making Security A Team Effort* by Carlos Mena, the observation is made that many organizations are now "moving to a single, enterprisewide approach to security, with a new goal: find the right balance between protective measures and acceptable risk."[2] HIPAA guidelines are designed to protect patient privacy and confidentiality; they therefore inherently encompass the entire organization. This enterprise wide approach is therefore appropriate. Since security is strongly tied to this goal, this approach promotes security implementation throughout the organization's many diverse digital systems and personnel.

Under the enterprise wide strategy the goal is to provide a central point of leadership while distributing the implementation. In the aforementioned article, reference is made to an 'enterprise-security group'. However, given the unique requirements of a healthcare organization, this group would be called the Enterprise

[2] Mena, Carlos. "Making Security A Team Effort"

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Privacy Group (EPG). As has been stated, the IPO job function is a requirement under HIPAA as stated in the *Standards for Privacy of Individually Identifiable Health Information*: "A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity."[3] This makes the IPO the best person to undertake the leadership role in the EPG.

The group should be comprised of personnel who are members of departments in the primary areas concerned with the implementation of HIPAA privacy and security guidelines. These would likely include, but not necessarily be limited to, members of Legal, Human Resources, Physical Security, Finance, and Information Technology. The ISO would be best suited to represent the Information Technology department in this group. The specific people chosen from each of the other departments would be those who are intimately aware of the functions and challenges within their respective departments.

From the outset, this group must have the will, support, and authority to get things accomplished. The simple legal mandates and recommendations of HIPPA are not sufficient. The organization as a whole, and more specifically those in executive positions, must provide the needed support to the group. In an interview with *Optimize Magazine*, author and consultant Thomas Parenty states:

> What matters is that whoever has that responsibility must be able to get something done, whether through the specific organizational position or, even more important, with the support of other executives. I've seen organizations where the chief information security person reports into building maintenance. I say, wonderful, have a CSO, but that's unimportant compared with the need for an individual who has the responsibility, the force of will, and the necessary support to do the job.[4]

This same concept applies to the Enterprise Privacy Group.

The primary responsibility of the group is to assess privacy risks under HIPAA guidelines, develop appropriate policy, and direct their implementation. The group would not exist for the goal of accomplishing a project. Rather, the job of this group would be perpetual. *Making Security A Team Effort* outlines:

> A four-step process: Identify risks, prioritize them, propose strategies, allocate resources to carry them out, and then validate those strategies and use what you've learned to start the cycle all over again.[5]

---

[3] U.S. Department of Health and Human Services Office for Civil Rights. "Standards for Privacy of Individually Identifiable Health Information Regulation Text; Security Standards for the Protection of Electronic Protected Health Information; General Administrative Requirements Including, Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings." Page 38 Section 164.530 (a)(1)(i)

[4] Parenty, Thomas. "Information Security: Beyond Firewalls."

[5] Mena, Carlos. "Making Security A Team Effort"

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

As a directly related function of this process, both physical and digital security would be actively addressed.

This group would directly report to the executives of the company. It would be in effect acting as the delegated agent of responsibility. They would define the priorities and budgeting for privacy/security expenditures and projects.

They would develop policies aimed at insuring the privacy of PHI. These policies would include certain security policies among them. However these would be general policies for organization wide implementation. The details of design and execution would be left to the departments under which the respective disciplines fell.

The Information Technology Security Group

Depending on the size of the department, the ISO alone will not be able to address all of the security needs and issues efficiently. Many larger Information Technology departments are segmented into groups or teams to handle different disciplines. For example, a team for desktop support, a team for network infrastructure, a team for Windows based servers; a team for UNIX based servers, and a team for Clinical Systems support. In a larger department there will need to be a person or persons specifically assigned to work with each of these teams in addressing security. These persons would in turn be members of an overall Information Technology Security Group (ITSG) within the department that would ultimately work under the direction of the ISO. This distributed model would allow the ISO to better address his/her primary tasks throughout the many diverse systems that are often found in a healthcare organization.

From the outset the ITSG should have a guiding mission statement. In light of HIPAA guidelines, it may look similar to this: 'To actively provide reasonable and appropriate measures to insure the security, integrity and availability of all information systems, services, and applications.' The purpose and goals for the team's existence must be clearly defined and understood by each of its members. To this end, it may be beneficial to create individual ownership by developing these goals with the active participation of each team member.

The ITSG should be the active force for maintaining security throughout the Information Technology department. They are charged with actively assisting the ISO in developing the detailed policies that support the general privacy and security policies defined by the Enterprise Privacy Group as it pertains to the Information Technology department. In many larger healthcare facilities, parties outside the department often make Information Technology decisions. This will be a particular challenge for the ITSG generally, and the ISO specifically. Vigilance will be required. The ITSG will have to address decisions that are made without their being consulted and, ideally, try to guide such decisions before they are made. This may require cultural shifts and underscores the need for support at the executive level. It also emphasizes the patience required by the ITSG members and their ability to affect progressive change while maintaining cooperation.

Each member of the ITSG would work with their assigned IT team or teams to support the defined policies and procedures. This would involve actively training the other IT staff in best practices, keeping them up-to-date with current threats and trends, working with new systems to ensure proper security implementation, and

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

constant evaluation of existing systems. Doing so would in turn require that each member of the ITSG is current with the aforementioned items.

Additionally, the individuals of the ITSG would work together to provide centralized solutions, wherever possible, to address security needs across IT teams. For example, one of the items required under the HIPAA Security Rule is Audit Trails. The ITSG may evaluate all possible means of maintaining this information and determine that a central SYSLOG server is the best solution. The members of ITSG would implement and maintain the central SYSLOG server. They would also work with their respectively assigned teams to ensure that all required systems are properly configured to send the required events and information to the central SYSLOG server. This commonality would provide reliability, standardization, and an overall efficient use of resources. This approach can have the added benefit of aiding risk assessment and incident handling.

One mistake made by many who start working in Information Security is an almost obsessive drive to lock down as much as possible. This should always be an underlying goal, but the ITSG must temper it with a number of realizations. First, it should be recognized that complete security is completely unattainable. This is especially true when first beginning the process in an environment that has historically given it little consideration. The HIPAA guideline itself directs 'reasonable and appropriate' as a driving motto. Second, while there is some pain to the end user when implementing security, especially where there was no or little security before, effort should always be made to minimize this. Third, security does not happen overnight. With so many challenges, time is needed to correct existing systems, change culture, and actively address new issues before they arise.

There are two methods for approaching security: Proactive and Reactive. The current state of many healthcare facilities will almost certainly place the ITSG into a reactive state. There may likely be a culture that reacts to incidents after their occurrence to prevent a reoccurrence, rather than taking steps to prevent the initial occurrence. Of course, the more desirable approach is Proactive; addressing security needs in advance of issues or incidents. In this approach the team is required to lock down existing systems in reaction to known vulnerabilities or potential issues. The goal of the team is to maintain operation in this mode. Much can be learned from operations in a reactive state, and this knowledge should be wisely put to use in making policy adjustments as well as future decisions. This of itself can be defined as being proactive.

Implementation

The remainder of this paper will discuss general approaches to specific security items utilizing the ITSG team approach. The direction put forth by the HIPAA Security Final Rule, as well as other generally held best practices will be used as a template for this discussion.

From the outset, the ITSG must be ever aware of the HIPAA mandate that PHI be safeguarded. The specifics of this demand, however, leave open for self-determination what is a reasonable level of safeguard. This was likely done due to the ever-changing nature of Information Technologies. It also places no requirements on systems that do not contain PHI. Therefore, a good rule of thumb will be for the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

ITSG to maintain general Information Security best practices. This will allow for the protection of not only PHI but all other information and systems as well.

Risk Assessment. A Risk Assessment should be done immediately. This can be undertaken either by the ITSG team or by an outside consulting firm. There is merit to both approaches. By having the ITSG team undertake the process, a more intimate knowledge of all systems and processes can be gained by its members. Alternatively an outside consulting firm with more experience may be in a better position to more thoroughly assess current risks.

HIPAA requires that Risk Analysis be done that evaluates the following major items.

Administrative Safeguards	Physical Safeguards	Technical Safeguards
○ Security Management Processes ○ Assigned Security Responsibility ○ Workforce Security ○ Information Access Management ○ Security Awareness and Training ○ Security Incident Handling ○ Contingency Plans ○ Periodic Re-evaluation ○ Business associate Contracts and Other Arrangement	○ Facility Access Control ○ Workstation Use and Security ○ Device and Media Controls	○ Access Control ○ Audit Controls ○ Data Authentication and Integrity ○ Encryption

But this Risk Assessment should not be limited exclusively to systems involved in PHI. Nor should it be restricted to the above outlined items. Rather, it should be a complete assessment of all systems that includes the above items.

Once the Risk Assessment is completed, the ITSG will need to review the results in relation to the HIPAA Security Standards as well as general best practices. Items requiring action be taken will need to be noted and a plan developed to do so. Using a reasonable and appropriate posture toward addressing discovered items, the ITSG will need to establish a prioritization scale to determine how best to address action items. This will involve determining how the affected systems are presently used, what is ideally needed to fully address the current security needs, what the implications are of reducing or delaying action, and how users and related systems will react to its implementation.

Security Policy. At the outset, policy must be established. Security policies will lay the framework for the work that the ITSG will do. As has been mentioned there will be general policies defined by the Enterprise Privacy Group. To these general policies, the ISO with the assistance of the ITSG will add specific security policies.

The beginning of defining security policies is to have a complete picture of the systems utilized throughout the organization. The risks posed by their existence and use must also be fully understood. This can likely be satisfied from the results of the Risk Assessment. Once this is established, processes common to multiple systems should be categorized as they relate to HIPAA Security Standards and security best

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

practices. From these categories policies can be created to address their respective security issues.

If the organization has a policy that defines the writing of policies, this must be adhered to when writing the security policies. Policies should be as concise as possible. They should also avoid overlapping other policies. Most importantly, care must be taken to avoid one policy conflicting with others. The security policies should address the various strategies utilized to address and manage risk. These will also address the recording, monitoring, and auditing of activities. Sanctioning policies may also be defined, though these will likely be addressed by the Enterprise Privacy Group in cooperation with the Legal and Personnel departments.

Those who will be charged with supporting, using, or enforcing security policies should review them. Finally, the policies must be reviewed and authorized for enforcement by the appropriate officers within the organization.

Training. A training regime should be developed around the security policies. This responsibility falls primarily to the ISO. As soon as possible training programs should be scheduled and held. An educated staff can greatly aid in maintaining a secure environment.

Under HIPAA guidelines, the entire workforce is to be included in the training programs. Ideally, as part of an orientation of new employees, an initial security training session should be held.

There are a number of items that should be covered in employee training sessions, some of which are mandated by HIPAA rules. Following are some items to be covered with the organization's workforce:

- Proper password management
- Physical Security awareness
- Awareness of social engineering tactics
- Responsible email usage and precautions
- Explanation of policies regarding the use of organization workstations

The medical staff in this regard can present a unique challenge for healthcare facilities. There are often physicians and other staff who are affiliated with, but not employed by, the organization. This may make them less inclined to attend training sessions and feel less bound by the policies put forth. Yet these individuals are often granted a high level of access to systems and, therefore, must be trained and held to established policy. In order to enforce this, as has been stated before, executive support is essential. Often there is an initial orientation that medical staff is required to attend; this would be an ideal situation to inject comprehensive security training.

More in-depth training should be addressed to IT staff. This includes staff that operates and supports clinical systems. In this area, the various members of the ITSG team can provide training geared toward the various systems used and supported by IT. This training would include areas of risk in given systems, maintaining security in interactions with vendors, general tactics used by attackers, and current threats.

As a healthcare facility's environment is ever changing and new threats are ever surfacing, a regular security bulletin process should be put into place. It has often been suggested that corporate email can be an effective tool for doing this.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

These bulletins can be sent out on a regular, while not excessive, basis to remind users of points covered in the awareness training, notify users of new security measures being implemented, and alerting them to current issues with a basic outline of any appropriate actions that should be taken. Additionally, the ITSG could consult with the Personnel department on other means they have found effective in communicating important information to all staff.

Implementation Plan. With policies established and a realistic view of the organization, the ITSG can undertake developing a plan to address action items. A target level of security should be established. This will be based on the findings of the Risk Assessment.

When evaluating the various action items, the team should establish a prioritization system based on the level of risk posed to a given resource. This will be used to determine how and when to address a given risk. This can be determined based on items such as:

- Known vulnerabilities of the item at risk.
- The quantity, distribution, and availability of means of exploitation of the item at risk.
- The level of availability of the resource at risk to users.
- The level of reliance by the organization on the resource at risk.
- The current status of the resources usable lifespan.
- The results to the organization and PHI should the resource's risk be exploited.

When determining the risk level of items, a secondary process would be to determine long-term plans. These long-term plans may include addressing low priority items or developing universal solutions to mitigate current high-risk issues. Within these plans it may be determined that revision of the security policies is appropriate.

A careful and deliberate study should be made. A practical security implementation will address security at multiple levels within the organization. The plan will start from broad safeguards like perimeter protection, moving to more focused safeguards like server protections, to focused safeguards like user access restrictions. By carefully evaluating the current risk assessment in light of a multi-leveled approach, common solutions can be developed. This is especially important given the many different systems often found in larger healthcare facilities. For example, a determination may be made that not all systems are capable of enforcing the required password and authentication policy. A cross-platform solution could be pursued for providing a single sign-on solution. This solution would address part of the Unique User Identification requirement and may also provide a means of monitoring systems login and providing necessary audit trails. This approach thereby allows the addressing of multiple HIPAA requirements via one solution encompassing multiple affected systems.

Care must be exercised to develop a plan that avoids costly or complex solutions. These pose a danger of actually negating any gains they may offer. A solution that is costly to implement may reduce needed resources for other areas. Additionally, solutions that are costly to maintain either monetarily or in terms of time

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

can lose value if these costs cannot be met. A complex solution can present difficulty in correctly implementing and maintaining; thereby reducing it's overall effectiveness. A complex solution may not have the ability to address the needs of all systems it may affect, and if not properly configured and maintained could introduce new risks.

It is important to remember that a secure solution may not require installing new systems. Since healthcare systems are at times implemented in a hasty fashion with the simply goal of getting them online, some of the built-in security features are not engaged. It may be possible to address items by simply implementing tools and functionality of an existing system. Alternatively, a restructuring of the implementation of a system or systems may be all that is required to attain the desired security level.

The ultimate plans should also aim to be as seamless as possible to the end users. The average user will not understand security requirements, and over utilizing HIPAA as an explanation for new measures can ultimately reduce it's impact as an argument for security. While training the users will assist in areas where they must be affected, there can be a tendency to challenge policies and systems that are confusing or burdensome to the users. This is especially true of healthcare providers who are more interested in caring for patients and associated tasks than having to deal with added security processes.

Once the implementation plans are developed, the individual projects must be planned. At this point, the various roles of each ITSG team member begin to diverge. Each team member will work with his assigned IT team to address their respective areas as required to achieve the target security level. Communication at this phase is essential. All parties required to work on the individual projects should be briefed on the goal and reason for each project. By so informing all project members, cooperation and communication regarding possibly unforeseen items of concern can be fostered.

Disaster Recovery Planning. The criticality of a Disaster Recovery Plan (DRP) cannot be overstated. Arguably, this is the highest priority item and should be developed immediately if the organization does not already have one. A good DRP is much more than tape backups, offsite storage, and copies of all major software. Developing and maintaining it will require the involvement of most, if not all, of the departments in the organization.

A DRP team must be created. The team will likely be managed by the ISO. A responsible person from each department should be included in the team. Since a large part of the work involves the IT department, as many members as possible should be included on the team. Like the ITSG, this team will become a constant feature of the organization. Once the initial DRP is developed, constant review, revision and testing will be required.

Having and maintaining a DRP is as much about an organization's culture as security is. While most will acknowledge its necessity, many will either discount the need for their own personal involvement or the urgency of developing the plan. A progressive cultural shift may likely be required in this regard. An aide to this will be having a member of each department on the DRP team. As they witness the large scope of the plan, each member will likely appreciate the very real need for the DRP.

The DRP team should proceed through the following four general phases:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Assess critical systems and define potential disasters
- Build and document a Disaster Recovery Plan
- Test the Disaster Recovery Plan
- Periodically review, revise and test the Disaster Recovery Plan

The team must be thorough in developing the DRP. Nothing can be taken for granted, especially since the plan is designed to respond to the loss of systems that are often taken for granted themselves. The plan must evaluate: what backup equipment should be kept available; where the backup equipment will be kept; how connectivity will be established to backup systems; how current data will be updated on backup systems; the sequence of activation of backup systems; what alternatives and processes to Information Systems the staff will implement.

In the initial development of the DRP, the team should sequentially go through the following procedures:

- Design a project plan with a timeline that will be adhered to with reasonable discipline
- Identify the critical systems and fully document them.
- Quantify possible disasters and identify the potential impact of each.
- Determine methods of mitigating any potential disasters and document.
- Identify roles to be filled in response to a disaster and the personnel to fill those roles.
- Develop and thoroughly document a plan to respond to the defined potential disasters.
- Implement mitigation actions where plausible.
- Thoroughly test the Disaster Recovery Plan.
- Make appropriate revisions.

Once the DRP is established it must remain relevant. This means regular evaluation, testing and revising where appropriate. Often disaster recovery planning is not included in healthcare systems projects. If newly implemented or upgraded systems are installed and not included in the DRP it becomes irrelevant. The members of the DRP team should take the lead in encouraging the inclusion of disaster recovery planning in new systems' project plans.

Incident Response. Incidents will occur. Processes and systems must be put into place and utilized to handle these. The goal is to provide a means to determine what has happened, what information to gather, with whom and how to communicate, and how best to react in order to prevent future incidents and restore systems.

In a healthcare facility, systems can generally be placed into two categories: general infrastructure or patient care related. The incident response plan may be tailored to address incidents that pertain to each type of system in different ways. For example, a part of the plan is to identify as much information about the degraded system as possible before attempting to repair and return it to service. This would be more feasible for a print server as opposed to a telemetry system, which would require restoration more quickly. Therefore, there may be effectively two procedural plans depending on the type of system affected by the incident.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The plan should outline who is a member of the incident response team. This will likely be members of the ITSG team and other key IT personnel qualified to assist in forensic and restorative functions. Also included may be clinical systems support staff, if appropriate to the incident. In the event of an incident, the team is contacted as the first order of business.

The plan should contain current contact information. This should be held for each incident response team member as well as any optional support staff required, including vendors, law enforcement, and other regulatory agencies. Within the plan should be a definition of 'how' and 'when' certain personnel are contacted regarding an incident. This would include criteria for determining whether to contact law enforcement or other regulatory agencies. Consideration should be given to when to contact law enforcement as there may be certain criteria that they will use for determining if the severity of the incident warrants their involvement.

The plan should outline the procedures to be followed in response to an incident. This should include steps to follow in gathering as much forensic information as possible before system restoration. As was mentioned, these might vary based on the type of system affected. The plan should include a procedure for implementing any backup systems available in order to preserve the affected system in its degraded state for analysis. There should be procedures for determining contributing causes to the incident. Findings from the investigation should be included in the current Risk Assessment so that they may be addressed through the other procedures already outlined.

As with other aspects of information security, the incident response plan should be regularly analyzed and updated where appropriate. A good practice is to review the successes and failures in following the plan in response to incidents. This allows the plan to be adapted to the unique culture and environment of the organization in order to be more effective in the future.

Conclusion

The tasks of the ISTG do not end with the completion of all plans and projects. Like any other system in Information Technology, the security systems put in to place need to be monitored and maintained. Incidents need to be identified and addressed. Awareness and response to the ever-changing threats must be maintained.

The overall process is in fact cyclical. HIPAA dictates that regular re-evaluations be done and this is generally held as best practice. Once the process has been completed, evaluation and improvement can be planned. Thus, the team returns to the Risk Assessment and begins the process again.

Information technology within healthcare organizations is quite complex and unique. Information Security within these organizations has now become a daunting task. However, it has also become an indispensable part of healthcare organizations. Implementing the organizational and procedural strategies outlined in this paper can assist in getting control of this necessary discipline. By following them, healthcare organizations can not only comply with HIPAA rules, but also gain active control of the security of their Information Systems. They can thereby successfully shift to implementing, and maintaining, a reasonable level Information Security.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of References

Amatayakul, Margret. “Rethinking Initial HIPAA Efforts.” November 2003. URL: http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_021660.html (14 Mar. 2004).

Brownlee, N. and Guttman, E. “RFC 2350 - Expectations for Computer Security Incident Response.” June 1998. URL: http://www.faqs.org/rfcs/rfc2350.html (12 Mar. 2004).

Cobb, Chey & Cobb, Stephen. “CISSP Comments on HIPAA Final Security Rule.” February, 2003. URL: http://www.privacyforbusiness.com/sources/HIPAAsecurityfinal_comments.pdf (12 Mar. 2004).

Darby, Christopher A.R. “Understanding Business Requirements: A Blueprint for Digital Security.” September 2002. URL: http://www.atstake.com/research/strategic_security/acrobat/atstake_security_blueprint.pdf (12 Mar. 2004).

Duffy, Daintry. “Security Planning: Don’t Press the Panic Button.” September 2001. URL: http://www.darwinmag.com/read/090101/panic.html (12 Mar. 2004).

Gartner, Inc. “Report: Building a Security-Aware Enterprise.” January 2002. URL: http://www.gartnerg2.com/site/FileDownload.asp?file=rpt-0102-0010.pdf (12 Mar. 2004).

Hoffman, Mark. “Dancing in the Dark.” September 2003. URL: http://www.darwinmag.com/read/090103/disaster.html (12 Mar. 2004).

Liu, Simon & Sullivan, John & Ormaner, Jerry. “A Practical Approach To Enterprise Security.” September 2001. URL: http://www.computer.org/itpro/homepage/Sept_Oct01/lui/print.htm (12 Mar. 2004).

Maiwald, Eric & Lyons, Barry. ”HIPAAsecurity: Assessments and Disaster Recovery Plans - Where to Begin?” URL: http://www.hipaadvisory.com/action/security/disasterrecov.htm

Mena, Carlos. “Making Security A Team Effort.” October 2002. URL: http://www.optimizemag.com/showArticle.jhtml?articleID=17700791 (12 Mar. 2004).

Parenty, Thomas. “Information Security: Beyond Firewalls.” December 2003. URL: http://www.optimizemag.com/showArticle.jhtml?articleID=17701015 (12 Mar. 2004).

U.S. Department of Health and Human Services. “45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule.” 20 February 2003. URL:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf (12 Mar. 2004).

U.S. Department of Health and Human Services. “Security and Electronic Signature Standards; Proposed Rule.” 12 August 1998 URL: http://aspe.hhs.gov/admnsimp/nprm/secnprm.txt (12 Mar. 2004).

U.S. Department of Health and Human Services Office for Civil Rights. “Standards for Privacy of Individually Identifiable Health Information Regulation Text; Security Standards for the Protection of Electronic Protected Health Information; General Administrative Requirements Including, Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings.” 17 April 2003. URL: http://www.hhs.gov/ocr/combinedregtext.pdf

© SANS Institute 2004, Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**