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.

Getting Started: The Impacts of Privacy and Security Under HIPAA - A Case Study

The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule went into effect on April 13, 2003 carrying with it security implications in the form of privacy safeguards. Late in 2002, a behavioral health agency realized that their use of a centralized electronic medical records (EMR) system and the requirements for HIPAA privacy had just accelerated their plans for security implementation. This paper is intended as a case study that can be applied in similar situations. It takes the reader t...

Copyright SANS Institute

Author Retains Full Rights

AD

Getting Started: The Impacts of Privacy and Security Under HIPAA
A Case Study

GIAC Security Essentials Certification (GSEC) Practical Assignment (V1.4b)
Option Two, Case Study in Information Security

Barbara Filkins
July 10, 2003

Abstract

April 13, 2003 was a landmark date for healthcare organizations through the United States. This is the day that the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule went into effect, carrying with it security implications in the form of privacy safeguards. Entities that limit their security planning and evaluation at this time, thinking that they have until April 21, 2005 to establish their HIPAA security practices, may be in for a shock. Full compliance actually requires an understanding and application of both rules, even with the scope of the final Security Rule now limited to electronic protected health information (PHI). An information security program must still consider physical security, since the HIPAA Privacy Rule (§164.530(c)) requires appropriate security for all PHI, regardless of the format or media.

Late in 2002, a behavioral health agency realized that their use of a centralized electronic medical records (EMR) system and the requirements for HIPAA privacy had just accelerated their plans for security implementation. This paper is intended as a case study that can be applied in similar situations. It takes the reader through the entire problem-solving process, starting with a situation assessment of the Agency's information management and technology resources. Along the way, the demands of the final Security Rule are explored and how they factor into the approach, touching on the intersections between it and the HIPAA Privacy Rule. The paper describes how the Agency established an on-going, cost-effective security program integrated with current Agency business practices.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Abstract 1
Introduction 3
The Before Snapshot – Of Situation Assessments and Gap Analysis 3
Focusing the Approach – HIPAA Security and Privacy Rule Considerations 9
HIPAA Security Standards 9
Security Standards: General Rules (§164.306) 9
Administrative Safeguards (§164.308) 10
Physical Safeguards (§164.310) 11
Technical Safeguards (§164.312) 12
Organizational Requirements (§164.314) 12
Policies and Procedures and Documentation Requirements (§164.316) 13
Intersections with the HIPAA Privacy Rule 13
Recommendations from Reviewing the Rules 15
Commitment, Organization, and Action! 16
Step One: Organize the Information 16
Step Two: Determine the Course of Action 20
Step Three: Establish A Security Management Program 21
Step Four: Review Agency Contingency Planning Documents 26
Step Five: Identify Key Security Policies 27
Step Six: Review and Update Business Associate Agreements 29
Step Seven: Security Training and Awareness 29
Step Eight: Technical Considerations 30
Impacts and Accomplishments 31
The After Snapshot -- Conclusions and Summary 34
References 35

Tables

Table 1: Definition of Remediation Options/WBS Activities 18
Table 2: Agency Remediation Findings Versus HIPAA Security Rule Requirements 19
Table 3: Security Team Membership 22
Table 4: OCTAVE^{sm} as Tailored by the Agency 25
Table 5: Agency Security Policy Framework 28

Figures

Figure 1: Representative Project Plan Schedule 20
Figure 2: HIPAA Documentation Tree 33

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction

In the fall of 2002, I was invited to join the consulting team that had been selected by a behavioral health agency, hereafter called the Agency, to provide a comprehensive HIPAA gap analysis and remediation strategy, including privacy, security, and transaction code sets. My role was to lead the security evaluation and provide a remediation strategy. Upon completion of the remediation planning, I was asked to continue as a consultant for the Agency to help them establish their security practice.

Although the Agency realized that they had roughly two years to prepare for the final Security Rule, they also acknowledged the current need to integrate information security into their current practices for a number of reasons. The Agency had developed a fairly sophisticated infrastructure based almost entirely on Microsoft products. They had invested heavily in the development of a centralized electronic medical record system that contains the mental, the medical, and the educational records of their juvenile clients. They were concerned about the possible sanctions imposed on them by the HIPAA privacy legislation, both from a business and a technical perspective. Being a non-profit agency, largely state and county funded, they were extremely cost conscious and needed to strategically plan their information technology investments, leveraging current staff and tools as much as possible.

All too often, security is marked as a 'special' technology, functionality, or set of business rules when in actuality it should be considered as part of normal operations. The Agency's goal was to establish an on-going, cost-effective security program integrated with the current business practices. This paper is intended as a case study and a roadmap for similar situations. It takes the reader through the entire problem-solving process, starting with a situation assessment of the Agency's information management and technology resources. Along the way, the demands of the final Security Rule are explored and how they factor into the approach, touching on the intersections between it and the HIPAA Privacy Rule. The paper outlines how a course of action was determined and concludes with the accomplishments to date and a brief summary of the results.

The Before Snapshot – Of Situation Assessments and Gap Analysis

A situation assessment is a term often used in strategic planning. It is a process of gathering and analyzing information needed to make an explicit evaluation of an organization and its environment. At the end of the assessment, a strategic planner will have a database that can be used in decision making and a list of critical issues that the organization needs to deal with in the planning process.

In this case, my challenges were to assess HIPAA security compliance across the entire Agency, propose a remediation approach, and develop an enterprise security strategy. I needed to develop an understanding of the entire Agency without which more detailed analysis would not be properly focused. I elected to conduct my evaluation of the agency's current security posture in a manner similar to how I would conduct a situation assessment. I then used the gap analysis to identify the critical issues.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

For the security situation assessment, I reviewed information about the Agency from three aspects -- organizational, technical (connectivity and systems), and information management (electronic and paper data). A summary of each follows.

Organizational: The Agency provides comprehensive family-centered, social, educational, and behavioral health programs for children and their families. They are involved in residential and day treatment programs, run two schools, and provide community based services. The Agency has non-profit status with funding sources that include the local county's behavioral health system, state Medicaid, federal, and private funding sources.

The workforce includes permanent employees, vendors, business associates (such as the legal counsel and IT vendors), volunteers, and interns. There are about 250 permanent employees and the retention rate is fairly high. All members of the workforce that have direct contact with the juvenile clients and all permanent employees undergo a stringent background check as part of the employment process and a lengthy probation period upon acceptance. Workforce IT skills are gradually improving commensurate with the growing dependence within the Agency on electronic information management.

During the course of this review, it became clearly apparent that security was going to involve the entire organization. Security-related activities were already distributed through out the Agency but there was no defined security support organization to address the emphasis that HIPAA placed on both the privacy and security of health-related information. Based on the business processes within the Agency, the core staff for security needed to include membership from the following departments:

- Information Management/Technology (IM/T). The information management (IM) staff is responsible for all electronic data as well as the clinical chart rooms, involving essentially all protected health information and associated records. The information technology (IT) staff manages the networks, the information systems, and all technical support services and operations.
- Human Resources (HR). The HR staff is responsible for all Agency workforce related issues, including training, awareness, and communication.
- Facilities. The staff manages the physical plant at each of the four main Agency sites, including responsibilities for maintenance records and emergency operations.

Additionally, the individual assigned to be the Agency's Chief Privacy Officer (CPO), required by the HIPAA Privacy Rule, needed to be included as a member of the security team.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Each therapeutic program within the Agency has specific requirements regarding security and privacy. However, individuals within these areas are not considered part of this corporate 'core' competency since their daily roles and responsibilities are not specifically oriented on establishing or maintaining security practices in the organization.

The Information Management/Technology Department is the obvious focus for the Agency's security organization. The culture of the organization is one of open communications and teamwork, making a security management program integrated with the Agency business practices quite practical and achievable.

Information Management: The Agency is transitioning from paper to a completely electronic environment for all their records. These include the medical, the mental health, and the educational charts for each juvenile client under Agency care.

When dealing with behavioral health issues, an increased level of privacy is required under both state and federal statues. Access to the medical and the mental health records for a client must be clearly separated and controlled strictly on a "need-to-know" basis. A medical doctor, for example, may be only authorized to see the medical history, not the mental health chart. Presently, the Agency concurrently manages both types of records in paper and electronic formats. This requires accurate tracking of who has authorized access to what type of record, who has accessed a record, when and for what purpose, and any unauthorized access to PHI.

The Agency has invested heavily in the development of an electronic medical records system. This is based on Microsoft SQLServer and is considered the Agency's most mission critical system. Housed at the headquarters, it is slowly becoming the central 'electronic' chart room for the Agency, containing all medical, mental, and educational records for all Agency clients. The Agency still relies on the original vendor design for system administration and audit capabilities. The use of this system generates both privacy and security concerns under HIPAA.

Information Technology: The Agency is an excellent example of steady, sustained growth. Management has planned wisely and has invested in solid technology to support their workforce. In 1995, they had a total of 10 computer systems at a single site. By 1999, this had grown to 7 servers and 140 systems across 7 sites. As of October, 2002, the agency had 21 servers and 315 systems (of which 150 are laptops) across 4 main sites and numerous secondary ones to include four group homes, several middle and high schools where the Agency provides services, and the home offices of key staff members who telecommute.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The administrative offices are at the heart of the network. The gateway router to the Internet is located here as is the Cisco 3015 Virtual Private Network (VPN) concentrator and the main Agency firewall. Dedicated point-to-point T1 lines connect the three main facilities (the residential campus, the community based services and day school, and the community based school) to the administrative office suite. The systems supporting the Agency's mission critical applications are located at headquarters.

All permanent locations are connected by the Agency's VPN. The Agency outsources the design, implementation, and management of their VPN to the telecommunications carrier who also supplies them with broadband and point-to-point services. At each fixed location, there is a Cisco PIX506 that provides the authentication into the VPN and establishes the encrypted tunnel through the VPN concentrator at headquarters. Additionally, single users, such as staff with mobile laptops, use a dialup connection via their Internet service provider (ISP) to the Citrix terminal server at headquarters. The VPN client is downloaded onto their machines.

From a system perspective, the Agency is fairly homogenous. When I started my review of their IT resources, the IM/T Department had just completed a migration of all desktops and servers to Windows 2000, establishing a pure Microsoft infrastructure at the operating system level and above. There are no immediate plans for migration to any newer versions. All application systems are either based on Microsoft products or being transitioned to them. Within the last six months, the IM/T staff has completed deployment of Active Directory and Windows 2K Group Policies, established a standard desktop configuration, and provided a new level of user management and administration capabilities.

The initial situation assessment revealed many security gaps, both technically and functionally. The Agency was on the verge of becoming overly dependent on their tools without really understanding where the holes in the technology might be and where they might be compromised. The need to comply with HIPAA privacy regulations had been a wake-up call. Management was now aware that even privacy had security implications and, like most healthcare organizations, was concerned and edgy over what the implications were.

The team identified numerous individual issues with the design and implementation of the Agency's infrastructure and systems, producing a 100+ page report. The major findings related to security are summarized below:

- *Audits and Alerts*. IM/T had not concisely defined what constitutes a "significant event" based on what they encounter in their review of system and network logs. The staff manually reviewed the logs from the Agency's over 20 servers on a weekly basis. Without auditing tools, this process is very error prone given the complexity of their operation. Workstations were also not routinely monitored or audited. Automated monitoring and alerting was essentially non-existent. The

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Agency basically did not have a proactive, automated capability to catch an incident in real-time.

- *Contingency and disaster recovery planning.* The Agency had developed a contingency and disaster recovery plan for the last JCAHO inspection over two years ago, but the document had not been updated commensurate with changes in their information systems and network. The plan also did not address any needed coordination between the IM/T, facilities, and other departments regarding availability to information, systems, communications, power, air conditioning, and key personnel in the case of an emergency.

- *Enterprise wide backup strategy.* The Agency performed daily, weekly, and monthly backups for their critical application servers, although the process was not centrally managed. They had a tape rotation schedule that provided for off-site storage and update of the backup tapes. Their backup strategy did not extend to user workstations where critical information may be resident, especially if service is abruptly suspended. They had not regularly tested whether their backups can be restored so there was low confidence in the overall process.

- *Facility and physical considerations for critical information systems.* The Agency had deployed many of their critical systems (e.g., records management, fund development, and human resources) with limited attention to availability, business continuity, or security concerns. Major application servers are located at headquarters. Configurations included RAID-5 disk systems, power protection, and hot swappable power supplies. They did not include fail-over modes or redundant systems at other Agency locations for availability, backup, or performance considerations, even as the Agency is moving towards operating their information systems on a 24 by 7 basis. The server room at headquarters lacked the sophistication needed for a growing organization. Cable management was missing. Servers were not rack mounted or even on shelves. The phone switch and patch panels were exposed to the non-IT vendors and vice versa. Due to lack of proper cooling capacity, the door was often left open and the room occasionally left unattended so that casual access by employees was possible.

- *Electronic Medical Record Security Management Capabilities.* The EMR system lacked robust security auditing or management capabilities. When the system was demonstrated to me, it was readily apparent that the capability of the system to set security settings for a user far exceeded its ability to audit these settings. An administrator could easily create highly customized group or user profiles from modifying a standard one. Yet there was no functionality that allowed them to collectively view the permissions they had set without retracing their original steps, a very cumbersome and error prone process. As a beta customer of the EMR vendor, the Agency needs to leverage their position and work directly with the system developers to understand and remedy the auditing issues for HIPAA security as well as improved system management and administration.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- *Infrastructure Management.* The Agency had various "ad-hoc" procedures and processes for managing their infrastructure and systems. They had not formalized them into an overall strategy for system and network configuration management that includes security as a key component. Procedures to evaluate and test infrastructure changes to the Agency's electronic information security baseline were non-existent.

- *Media Control.* The Agency lacked any centralized control over the movement of their electronic system assets. They used hand receipts, charged back to an employee's department, to track the movement of hardware, software, and media. The Agency does follow rigorous procedures for the disposal of media, ensuring that hard disks are permanently cleansed of all information before they are released from the Agency.

- *Organization.* The Agency has committed to overall HIPAA compliance as documented in their Strategic and Operational Plans. They had developed an organizational structure for privacy. They had not appointed a Chief Security Officer (CSO), defined the CSO duties, and established one or more security support teams.

- *Policies and Procedures.* The Agency had implemented numerous security procedures, such as strong passwords, use of password-protected screensavers, and automated logouts after a specified time. However, their documentation did not match what they had implemented. Additionally, workforce members within various departments had created local procedures that potentially conflicted with an Agency policy. Formal documentation of policies and procedures for handling either electronic or paper-based health information did not exist within the Agency nor did an overall formal management review and approval process for policies, guidance, or procedures.

- *Security Training and Awareness.* The Agency workforce receives basic privacy and security training as part of the new employee orientation and during the actual probation period when "on-the-job" training is conducted. The Agency has not developed any formal guidelines or requirements for on-going security awareness. The extent to which the Agency requires security training and awareness of contractors and vendors was not clear. Workforce skills relative to information technology were not routinely evaluated to ensure that individuals understood and could comply with the technical aspects of electronic information security.

The Agency Chief Information Officer (CIO) was aggressively working towards a very elegant, state-of-the-practice, network-based environment for information management. Once aware of the many issues facing him, he actively wanted to resolve them, but was heavily constrained by resources and dollars. His vision of pushing off HIPAA security until closer to the compliance date of April 21, 2005, quickly evaporated as I started to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

present the results of the situation assessment along with my analysis of HIPAA requirements.

Any release of PHI, whether accidental or intentional, represents potentially significant liability to the organization. The absence of an entity-wide security organization, established procedures specific to security, and automated auditing and monitoring tools placed the Agency in a vulnerable position of not even being able to detect when a possible breach to its information systems occurred. The CIO quickly realized that, given Agency dependence on electronic PHI, security required an immediate focus because of privacy safeguards.

The Agency identified the critical issues as:

- An increasing reliance on technology without understanding the inherent vulnerabilities and possible compromises to Agency business operations.
- The realization they could not postpone any further the integration of security into their current IM and IT operations because of their use of electronic PHI and the HIPAA Privacy Rule.
- The lack of knowing what the major risks really were as no risk analysis had been performed.
- Prioritization of the functional and technical information security requirements.
- The lack of an organizational framework for the implementation and management of Agency security practices.
- The wise management of security implementation resources and costs.

The Agency needed not only the roadmap to establish their security practices, but also the plan for how to allocate needed resources, services, and tools that took into account the tradeoffs between cost and risk mitigation.

Focusing the Approach – HIPAA Security and Privacy Rule Considerations

My next step was to review the HIPAA Security Rule in depth, correlate it with Privacy, and discern any specific impacts prior to providing further recommendations to the Agency.

HIPAA Security Standards

The final HIPAA Security Rule, published in the Federal Register on February 20, 2003, outlines the security standards, implementation standards, and requirements with which all covered entities (i.e., health plans, health care providers, and clearinghouses) must comply with respect to electronic protected health information. This section gives synopsis of the final rule. Each major section is summarized with a brief discussion included as to its potential impact on an entity's security practices.

Security Standards: General Rules (§164.306)

Section §164.306(a) states:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under [the Privacy Rule].
(4) Ensure security compliance with this subpart by its workforce (Federal Register, vol. 68, no. 34, 8376).

Note that §164.306(a)(3) states one of the major intersections between the two rules – the Privacy Rule is key to determining the business rules that the Security Rule must support.

An entity can develop a flexible approach to their implementation of security, establishing reasonable and appropriate measures to meet the standards (i.e., the requirements) and the implementation specifications, the instructions for implementing these standards (Federal Register, vol. 68, no 34, 8336). The analysis must show that the agency has taken certain factors into consideration such as their environment, their capabilities, and the cost.

Certain implementation specifications, such as encryption, are designated as "addressable" -- an entity may elect not to implement those specifications or implement an alternative. However, the entity must clearly document their analysis of whether their implementation decisions meet the key elements of "reasonable and appropriate". Logically, this should be done during the risk analysis required by §164.308(a)(ii)(A) with the decisions documented as part of those outcomes. The entity must also review this information and update it "as needed" to ensure continued protection of electronic PHI. The rule does not specify the interval, but the entity should follow best practices such as:

- Annually as part of an overall evaluation of the security practices.
- Occasionally whenever a change to privacy or security policy is indicated, such as by an increasing number of the same potential or actual incidents.
- Naturally whenever a change in the operational environment affecting electronic information occurs, such as major upgrades to the IT infrastructure.

Administrative Safeguards (§164.308)

According to the definition of administrative safeguards in §164.304, a covered entity must establish the "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of the security measures to protect electronic protected health information and to manage the conduct of the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

covered entity's workforce in relation to the protection of that information" (Federal Register, vol. 68, no. 34, 8376).

This section lays the basis for the Security Management Program proposed in this paper. Specific standards and implementation specifications include: risk analysis, risk management, an established sanction policy, and information system activity review; identification of a chief security officer; procedures for workforce management and supervision, personnel clearance, and termination; information access management, including access authorization, establishment and modification; workforce training and awareness including procedures for password management, malicious code protection, security reminders, and log-in monitoring; security incident procedures including response and reporting; contingency plans that cover data backup, disaster recovery and emergency mode operations; and the need to establish periodic evaluations, both technical and non-technical, for security related activities. This section continues the emphasis placed on risk analysis in §164.306 and specifically calls for an applications and data criticality review to be performed in support of contingency planning. Logically, this last activity should also be part of the risk analysis that the entity is required to undertake.

This rule also establishes the requirement for a written contract between the entity and any business associate who creates, receives, maintains or transmits PHI on the covered entity's behalf. "Other arrangements" are also referenced but these are later clarified in §164.314 as applicable to either covered entities and business associates that are both governmental agencies or relationships between an entity and a business associate that are required by law, i.e., not wholly elective on the part of the covered entity (CE). Regardless, the business associate must provide satisfactory assurance that they will appropriately safeguard the CE's information.

Physical Safeguards (§164.310)

According to the definition of physical safeguards in §164.304, the covered entity must establish the "physical measure, policies, and procedures to protect their electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion" (Federal Register, vol. 68, no. 34, 8376).

This section of the rule states the facility requirements with an emphasis on securing physical access and protecting data. Facility has been defined as the "physical premises and exterior and interior of a building" (Federal Register, vol. 68, no. 34, 8340). In §164.310, the term takes on a specific reference to the buildings housing the information systems of the entity (Federal Register, vol. 68, no. 34, 8378). The rule establishes requirements for: facility access controls, including contingency operations, establishing a facility security plan, access control and validation (e.g., visitor control procedures), and the documentation of any security-related facility maintenance; workstation use and security; and device and media controls dealing with the movement of hardware and electronic media containing PHI throughout the entity's facilities, procedures for the proper disposal and re-use of media, record keeping (i.e., inventory

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and tracking) to establish accountability for hardware and media, and backup and storage procedures in the event of equipment movement.

Based on this section of the rule, an entity should incorporate facility planning into both its initial risk analysis as well as its on-going risk management activities. The security team must include membership from the facilities department. Consideration needs to be given to the fact that hardware "systems" actually decompose into their physical components, such as monitor, peripherals, CPU, and disk subsystem(s). Hard drives containing PHI can readily be separated from the servers or workstations that contain them. The inventory and tracking system should track these storage devices, both configured within a larger system and individually.

Technical Safeguards (§164.312)

According to the definition of technical safeguards in §164.304, the covered entity must implement both the "technology and the policies and procedures for its use that protect electronic protected health information and control access to it" (Federal Register, vol. 68, no. 34, 8376).

This section of the rule outlines the technical standards for: access control, including unique user identification, emergency procedures for access to electronic PHI, automatic logoff, and encryption of electronic PHI; audit controls; information or data integrity including authentication mechanisms to ensure against the alteration or destruction of data in an unauthorized manner; person or entity authentication; and transmission security including integrity controls over and encryption of the electronic PHI in transit.

Most of the implementation specifications that accompany the technical standards are addressable. For example, encryption is in the addressable category. Based on the definition of "reasonable and appropriate" in section §164.306, an entity may elect not to implement the addressable specifications. However, the burden of proof is upon the entity to demonstrate that they either do not need to implement that specification and/or that they have an acceptable alternative. In my opinion, this again emphasizes that an entity must have a strong risk analysis, an acceptable level of documentation from that process, and a demonstrable, on-going risk management program that supports continuous process improvement and on-going evaluation of its security activities in light of its business objectives.

Organizational Requirements (§164.314)

This section of the rule delineates the contractual requirements (i.e., terms and conditions) for a business associate that is involved with the creation, receipt, maintenance or transmission of electronic PHI on behalf of the entity. Under the requirements of this section, an entity must take corrective action if they are aware of a pattern of activity or practice that would constitute a material breach or violation of their business associate's contractual obligation. If corrective action is not feasible, then the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

contract must be terminated by the entity. The contract between the entity and the business associate must have a termination clause that supports this action.

The Government realizes that there are some relationships an entity must enter into as required by law. For example, the Agency has a contract with the local county's Department of Behavioral Health Services to provide care to juvenile wards of the county. In this case, the contractual requirements do not apply but there is still the responsibility on behalf of the Agency to take corrective action if they perceive that there is an issue. In this case, if correction is not possible, the Agency must report the problem to the Secretary of Health and Human Services (HHS).

Policies and Procedures and Documentation Requirements (§164.316)

The rule requires that an entity implement policies and procedures (P&Ps) outlining how they will comply with the standards, implementation specifications, and other requirements of the Security Rule. From a review of the entire rule, documentation will include: risk analysis results, audit logs, access reports, security incident reports and outcomes, policies and procedures related to security, contracts with business associates, facility maintenance records, device and media accountability and tracking records, media disposition and tracking records. Some of this information will contain electronic PHI and be subject to additional privacy and confidentiality regulations.

Both P&Ps and any other required records from an action, activity, or assessment must be maintained in written (including electronic) format for 6 years from the date of creation or the date of implementation, whichever is later. The information must be readily available to the workforce responsible for implementation of the procedures. The information must be reviewed and updated on a periodic basis, whether yearly or whenever the entity incurs changes in its operational processes, infrastructure, or environmental needs.

Intersections with the HIPAA Privacy Rule

The final version of the Security Rule is closely aligned with privacy and supports the increasing use of electronic information in the healthcare industry. It provides standards and implementation specifications for basic safeguards to aid against unauthorized access, alteration, deletion, or transmission of electronic PHI. The Privacy Rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information (Federal Register, vol. 65, no. 250. 82827).

The major overlaps between the two rules are:

- *Appropriate and reasonable safeguards:* Both the Security and Privacy Rules require covered entities to take appropriate and reasonable measures to safeguard protected health information. Both require an entity to assess and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

define its needs, select and implement protections appropriate for its own environment, and balance risk and remediation cost.

The Privacy Rule applies to protected health information in any form. Section §164.530(c)(1) states the general mandate to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information" (Federal Register, vol. 65, no. 250. 82462). Thus, even without the security regulation, HIPAA already mandates covered entities must keep health information secure. The best approach to demonstrate that the safeguards in place are appropriate to meet the privacy mandate is to comply with the Security Rule.

- *Mapping PHI flows:* To comply with both rules, an entity must list its PHI and map its movement both internal and external to the organization. Understanding the PHI flow is necessary to identify uses and disclosures and implement appropriate safeguards.

- *Protecting PHI:* Identifying all individually identifiable health information, in any form, will help define the security responsibilities of the agency. All PHI must be appropriately protected by policies, procedures, and security measures, both physical and technological.

- *Limited access (minimum necessary/need to know):* Both rules require that access to PHI be restricted. The Privacy Rule requires that use of PHI be based on employees' job roles (i.e., role-based access). This means that an entity must identify the types of employees that need access to PHI and the specific PHI needed (Federal Register, vol. 65, no. 250, 82819). In the final version of the Security Rule, role-based access was removed as a standard but, considering the implications of both rule relative to electronic PHI, the security mechanisms selected to enforce access limitations should be role based.

- *Third-party (i.e., business associates) agreements:* The two rules have become more aligned in this area with the final version of the Security Rule. Both privacy and security provisions must be passed on to business associates via contracts to ensure that PHI is protected at all times. An entity is also required to act on any knowledge that a business associate may not be complying with those provisions.

- *Accountability:* Both rules require that someone be assigned to assure that PHI is adequately protected. For privacy, this is the Chief Privacy Officer. For security, this is the Chief Security Officer. The two positions, however, are very symbiotic in nature, overlap in several areas, and should be coordinated in practice.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- *Training and awareness:* Both rules require regular training to make certain all employees understand the importance of protecting PHI and how they must do so.

Recommendations from Reviewing the Rules

Based on my review of the rules, I came up with the following recommendations for the Agency:

1. The establishment of a formal *security management process* is essential to the compliance with §164.308. For this, I proposed a security management program be established, documented by a formal plan. The program would "involve the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations. This [program] would include implementation features consisting of a risk analysis, risk management, and sanction and security policies" (Federal Register, vol. 68, no. 34, 8346).

2. The *risk analysis and risk management processes* required by §164.308 are critical to defining the measures against which the Agency's implementation of HIPAA security would be assessed. Additionally, other sections of the rule re-emphasize the criticality of a strong, well-documented risk analysis. Therefore, the development of demonstrable risk analysis and management processes was flagged as a priority for the Agency.

3. Because of their use of electronic PHI, *establishing "reasonable and appropriate" privacy safeguards* also meant that the Agency needed to implement the appropriate security safeguards. Otherwise, they could face simultaneous violations of both rules. For example, disclosure of electronic PHI to an unauthorized party, such as two users sharing their account username and password to the EMR, would be in direct violation of both the HIPAA Security and Privacy Rules. The Agency needed to develop a security requirements database to demonstrate their determination of what is "reasonable and appropriate".

4. The Security Rule is *documentation* intensive. According to the Government, "the standards do not allow organizations to make their own rules, only their own technology choices" (Federal Register, vol. 68, no. 34, 8343). The Agency must demonstrate how they comply with all the requirements of this rule, including justification for their implementation decisions and how effective their decisions are. The documentation requirements for security parallel those for privacy. The Agency privacy and security teams need to work together to develop a document management process that supports both rules.

5. The Agency needs to develop sanctions for *non-compliance with privacy,* coordinating with those under development by HHS. I have seen several references in the media that the final Security Rule will very likely be used as

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

guidance in cases where privacy violations involving electronic PHI have occurred. I also anticipate that review of any Agency privacy incident or violation will include an in-depth review and assessment of the Agency's security risk analysis, implementation documents, including their analysis of "reasonable and appropriate", and other artifacts such as audits, incident reports, and corrective actions. The Agency needs to establish a *quality framework for security* based on objective metrics and indicators. They then need to collect the data and demonstrate how this data measures the quality of the security management program.

6. The Agency has outsourced several critical IT services, including the VPN design, implementation, and management, hardware maintenance, and telephone switch support. These vendors are either directly involved in the transmission of PHI or indirectly in its handling. Existing contracts or service level agreements (SLA) may be sufficient but need to be reviewed against the requirements of §164.308 and §164.314 to ensure that the proper *contractual terms and conditions for business associates* are contained in those documents.

Commitment, Organization, and Action!

The CIO was committed to implementing a sound security program based on these recommendations. Together, we established two key guiding principles:

1. The scope of the project had become enterprise security at a very broad and complex level. An enterprise-wide strategy was needed, essentially recreating the IM/IT fabric of the organization to integrate privacy and security into the Agency's mission and business objectives.
2. The project must be quantified into affordable activities that could be scheduled and prioritized. Planning had to account for all cost and resource considerations.

I developed a methodology to address the complex set of issues, threats, vulnerabilities, and risks identified by the consulting team during the initial project's data collection. I established the approach outlined below, using the knowledge I gained from the topics in the SANS Security Essentials course, my own background in system engineering, and the structure of the HIPAA Security Rule.

Step One: Organize the Information

Data collection for the gap analysis had been guided by a questionnaire organized into the six main areas of the rule. The questions reflected the HIPAA standards and industry best practices for security. Each had a Yes/No/Not Applicable column, backed by a narrative description. Key Agency staff members were surveyed and the results compiled into a small database. These results, together with my analysis of the security posture of the organization, provided copious amounts of data with which to work. The challenge was organizing and presenting information in a meaningful fashion.

I defined ten (10) basic remediation categories that could be used to help close the security gaps. These options reflected regulation requirements, industry best practices,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and the use of information technology at the Agency. Each category was further described by a standard set of activities easily defined as elements of a Work Breakdown Structure (WBS), described and prioritized as shown in Table 1. I devised a simple weighting scheme to demonstrate full compliance, partial compliance, or no compliance with the HIPAA Security Rule. This approach allowed the presentation of the gap analysis results in matrix format that summarized each section of the rule, demonstrated where the associated gaps occurred, and indicated what the applicable remediation option(s) were. Table 2 presents the results of the Agency gap analysis, captured in matrix format, and compared against the WBS activity descriptions.

The Agency used this matrix to quickly review where their security gaps existed, tailored the activities under each remediation option to their specific needs, and developed a project plan for HIPAA security compliance. Assumptions were established from the survey narratives associated with each gap, a WBS was entered into Microsoft Project, and a schedule developed. This allowed task dependencies to be identified, resources assigned, needed tools established, and costs itemized by WBS activity and time, all through the capabilities of Project.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 1: Definition of Remediation Options/WBS Activities

WBS Element	Remediation Option	WBS Activity Description (Brief)	Security Rule Reference
1	**Security Management Program**	Formal and central management structure that creates, administers, and oversees security related policies and procedures to ensure the prevention, detection, containment, and correction of security breaches	§164.306 §164.308(a) - all §164.308(a)(1) §164.308(a)(2) §164.308(a)(6) §164.310(a)(1)
2	**Business Continuity Planning and Disaster Recovery**	Contingency planning to respond to a system emergency or disaster. Plans must be formally documented and periodically tested	§164.308(a)(7) §164.310(a)(2)(i)
3	**Policies and Procedures**	An organizational framework that establishes needed levels of information security and privacy to achieve the desired confidentiality goals	§164.316 All related parts of rule that refer to P&Ps
4	**Human Resource Policies and Procedures**	Personnel security and other security related aspects of dealing with employees	§164.308(a)(3)
5	**Business Associate Agreements**	Contract between two business partners for the electronic exchange or handling of data, protecting the integrity and confidentiality of the data exchanged or handled	§164.308(b)(1) §164.314
6	**Security Training and Awareness**	Education of the entity workforce regarding security and the reinforcement of that education through on-going reminders to create security awareness as part of the daily responsibilities in the organization	§164.308(a)(5)
7	**System / Network Technical Architecture**	Standards based architecture that addresses security issues and mitigates risk while meeting entity business and functional needs and requirements	§164.312 - all
8	**Evaluation**	Technical evaluation to establish the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements	§164.308(a)(8)
9	**System / Network Management & Administration**	Standardized functions and services standardized applied uniformly through out the organization, centrally managed, and support to capacity planning and management operations	§164.310(d) §164.312(b)
10	**User Management, Support & Outreach**	Management and support of the end-user environment, incorporating security requirements into the entities IT support structure, such as through user interactions with the helpdesk and on-line knowledge bases	§164.308(a)(4) §164.308(a)(5)(i)(B)-(D) §164.310(b) §164.310(c) §164.312(a)

Figure 1 shows a provisional schedule that was developed from the tailored WBS description. This tool was used to generate several different scenarios. Each scenario could be evaluated based on resources used and cost. The final version, not shown here, was used to substantiate the budget request for additional resources (staff, tools, and dollars).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Gap Analysis / Remediation Categories WBS Element	Security Management Program (WBS 1.0)	Business Continuity & Disaster Recovery (WBS 2.0)	Policies and Procedures (WBS 3.0)	Human Resources Protection (WBS 4.0)	Business Associate Agreements (WBS 5.0)	Training (WBS 6.0)	Incident Reporting (WBS 7.0)	Evaluation (WBS 8.0)	Physical Safeguards Implemented (WBS 9.0)	User Management (WBS 10.0)
Administrative Safeguards										
Security Management Process	▲		✓					✓		
Assigned Security Responsibility				●						
Workforce Security				▲						
Information Access Management	▲			▲			✓		✓	✓
Security Awareness and Training	▲		✓							✓
Security Incident Procedures	○	✓					✓			✓
Contingency Plan	▲									
Evaluation	○	✓					✓		✓	
Business Associates Contracts	▲				✓				✓	
Physical Safeguards										
Facility Access Controls	▲	✓								
Workstation Use	▲		✓							
Workstation Security	▲		✓				✓			
Device and Media Controls	▲	✓	✓						✓	
Technical Safeguards									✓	
Access Controls	▲						✓		✓	✓
Audit Controls	○								✓	✓
Integrity	●									
Person or Entity Authentication	▲		✓				✓		✓	
Transmission Security	▲							✓	✓	
Organizational Requirements										
Business Associate Contracts or Other Arrangements	▲				✓					
Policies & Procedures & Documentation Requirements										
Requirements for Group Health Plans	N/A									
Policies & Procedures & Documentation Requirements	▲	✓					✓		✓	

○ = No Compliance ▲ = Partial Compliance ● = Full Compliance N/A = Not Applicable

Table 2: Agency Remediation Findings Versus HIPAA Security Rule Requirements

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ID	WBS	Task Name	Duration	Start	Finish
1	1	WBS 1: Security Management Program	295 days	Mon 12/9/02	Fri 1/23/04
2	1.1	1.1 Establish Organizational Structure	10 days	Mon 12/9/02	Fri 12/20/02
3	1.1.1	Define Staff	10 days	Mon 12/9/02	Fri 12/20/02
4	1.1.1.1	Appoint CSO	1 day	Mon 12/9/02	Mon 12/9/02
5	1.1.1.2	Define Roles and Responsibilities	2 wks	Mon 12/9/02	Fri 12/20/02
6	1.1.2	Establish Reporting Structure	10 days	Mon 12/9/02	Fri 12/20/02
7	1.1.2.1	Normal Procedures	2 wks	Mon 12/9/02	Fri 12/20/02
8	1.1.2.2	Incident Reporting	2 wks	Mon 12/9/02	Fri 12/20/02
9	1.2	Risk Assessment / Management	60 days	Mon 1/6/03	Fri 3/28/03
10	1.2.1	Develop risk assessment inventor	40 days	Mon 1/6/03	Fri 2/28/03
11	1.2.1.2	Define assets, category, and valu	1 mon	Mon 1/6/03	Fri 1/31/03
12	1.2.1.3	Establish security classification	2 wks	Mon 2/3/03	Fri 2/14/03
13	1.2.1.5	Determine threats (method, likeliho	1 mon	Mon 1/6/03	Fri 1/31/03
14	1.2.1.6	Determine potential cost of securit	1 mon	Mon 1/20/03	Fri 2/14/03
15	1.2.1.7	Evaluate asset value vs. security	2 wks	Mon 2/17/03	Fri 2/28/03
16	1.2.2	Develop risk management strategy / tra	1 mon	Mon 3/3/03	Fri 3/28/03
17	1.3	Develop Entity-Wide Security Plan	90 days	Mon 12/9/02	Fri 4/11/03
35	1.4	Approved Plan	50 days	Fri 1/31/03	Fri 4/11/03
36	1.4.1	Draft	0 days	Fri 1/31/03	Fri 1/31/03
37	1.4.2	Final	0 days	Fri 4/11/03	Fri 4/11/03
38	1.5	Security Program Management Review	199 days	Wed 3/5/03	Mon 12/8/03
48	1.6	Security Plan Update Process	25 days	Mon 12/22/03	Fri 1/23/04
50	2	WBS 2: Business Continuity and Disaster R	232 days	Mon 12/9/02	Tue 10/28/03
51	2.1	Analysis and Preparation	35 days	Mon 12/9/02	Fri 1/24/03
66	2.2	Plan Creation and Approval	21 days	Fri 1/31/03	Fri 2/28/03
70	2.3	Testing and Update	12 days	Mon 10/13/03	Tue 10/28/03
75	3	WBS 3: Policies and Procedures	265 days	Mon 12/9/02	Fri 12/12/03
76	3.1	Identification of All Areas that Require Polici	1 wk	Mon 12/9/02	Fri 12/13/02
77	3.2	Formal documentation of policies and proce	3.5 mons	Mon 1/6/03	Fri 4/11/03
78	3.1	Approved Set of Security P&P	0 days	Fri 4/11/03	Fri 4/11/03
79	3.3	Evaluation	198 days	Thu 3/6/03	Mon 12/8/03
87	3.4	Review and Update	201 days	Fri 3/7/03	Fri 12/12/03
95	4	WBS 4: Human Resources	40 days	Mon 12/16/02	Fri 2/7/03
96	4.1	Review of existing procedures	1 mon	Mon 12/16/02	Fri 1/10/03
97	4.2	Updates based on evaluation	1 mon	Mon 1/13/03	Fri 2/7/03
98	5	WBS 5: Chain of Trust Agreement (CoTA)	35 days	Mon 12/9/02	Fri 3/7/03
103	6	WBS 6: Training and Awareness	287 days	Mon 12/9/02	Tue 4/13/04
145	7	WBS 7: System Technical Architecture	140 days	Mon 12/9/02	Fri 6/20/03
168	8	WBS 8: Certification	204 days	Mon 2/3/03	Thu 11/13/03
170	8.1	Internal Review	4.5 mons	Mon 2/3/03	Fri 6/6/03
171	8.2	Independent Assessment / External Review	1 mon	Mon 6/9/03	Fri 7/4/03
172	8.3	Auditing	94 days	Mon 7/7/03	Thu 11/13/03
173	8.3.1	Auditing 1	1 wk	Mon 7/7/03	Fri 7/11/03
174	8.3.2	Auditing 2	1 wk	Fri 11/7/03	Thu 11/13/03
175	9	WBS 9: System / Network Management	295 days	Mon 12/9/02	Fri 1/23/04
176	9.1	System / Network Configuration Proce	40 days	Mon 12/9/02	Fri 1/31/03
179	9.2	Development of Security Elements for	140 days	Mon 12/9/02	Fri 6/20/03
180	9.3	Network Management and Monitoring	156 days	Mon 5/26/03	Fri 1/23/04
371	9.4	System / Network Management Review	200 days	Tue 3/4/03	Mon 12/8/03
372	10	WBS 10: Asset Management Support	202 days	Mon 12/9/02	Wed 4/7/04

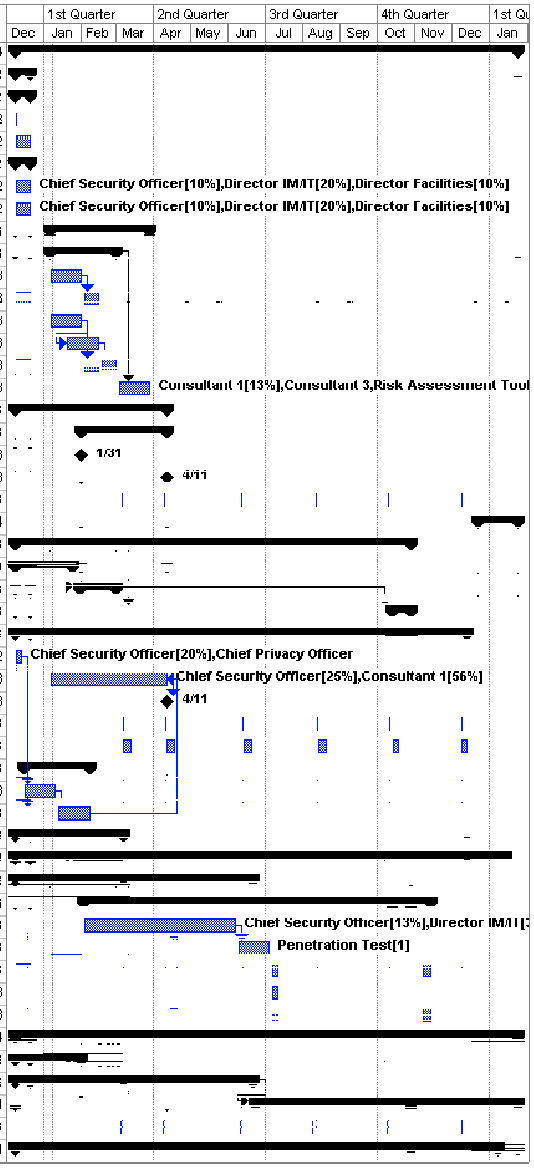

Figure 1: Representative Project Plan Schedule

Step Two: Determine the Course of Action

The CIO and I determined that the Agency needed to spend the remainder of the first year establishing the foundation for a sound security practice. The Agency was constrained by the fact that the fiscal year (FY) 2003 operating budget had already been established. Any major investment, such as the purchase of enterprise products for policy compliance, vulnerability management, or automated system and network auditing and alerting, would need to be approved as part of the FY 2004 budget.

The actions were prioritized as follows:

1. Establish a security management program, including risk analysis and risk management.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2. Review Agency contingency planning documents.
3. Identify key security policies.
4. Review and update business associate agreements related to IT.
5. Establish security training and awareness program.
6. Focus on the technical considerations.

Step Three: Establish A Security Management Program

Planning and assessment are at the foundation of a successful security program. Planning is essential to establish organizational responsibilities and define the necessary communication processes before an incident occurs. *Proactive* planning measures will reduce, if not eliminate, the risk of exposure (Benson). *Reactive* planning measures, however, are still needed since it is impossible to address all contingencies (Benson). Business continuity planning in the face of a potential natural disaster is one such example. Assessment, however, is the second critical element. Proper and thorough planning for security may not be achieved without a full risk assessment being performed along with an associated cost/benefit evaluation.

The first step in the proposed course of action was to establish the Security Management Program. A security management program encompasses the "creation, administration and oversight of policies [and procedures] to ensure the prevention, detection, containment, and correction of security breaches". It involves risk analysis and risk management, including "the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of organizational assets (both physical and electronic)" (Federal Register, vol. 63, no. 155, 43267). This program was to be integrated with the organizational and management structure of the Agency, as opposed to being considered a separate department within the Agency.

The following activities were completed:

Establish the organizational structure. The Agency determined the security roles and responsibilities within their organization, including the Chief Security Officer and supporting staff. Roles were designated that address both physical and electronic information security. A reporting structure was developed both for 1) routine operations, normal problem reporting and standard escalation procedures, and 2) incident reporting and emergency response procedures. This information was documented in the Security Management Plan and will be continually updated as needed by the program.

Table 2 demonstrates how the security organization crosses Agency organizational boundaries. Three teams were formed, based on the list of common computer security incident response services outlined in the Handbook for Computer Incident Response Teams, published by Carnegie-Mellon Software Engineering Institute (SEI) (West-Brown et al. 24-5).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1) The *Operational Security Team* is responsible for routine protection of the agency's electronic information. The services that this team provides are proactive, intended to reduce the number of future incidents.
2) The *Rapid Response Team* is responsible for emergency or priority matters and includes incident handling services. The services this team provides are reactive in nature, triggered by an event or request that may become an incident.
3) The *Security Quality Management Team* is responsible for defining and managing key security processes and analyzing and acting on all information. This team is also responsible for conducting the security risk assessment and analyzing its outcomes.

Table 3: Security Team Membership

Functional Area / Department	Role/Responsibility	Team Membership			Title
		Operational	Rapid Response	Quality Management	
IM/T	To include data/information, user management and network/system	X X X	X X X	X X X X	Network Director Network Manager Security Technician Director of Database Service Director of Charts & Records
HR/Training	To include security awareness and training			X	Director of Staff Development
Privacy	To provide coordinate between privacy and security activities within the agency			X	CPO
Facility	To provide required coordination between physical and IT security	X	X	X	Director Facilities Manager Facilities
Management		X	X	X X X X	COO VP of Programs VP of HR CSO

Establish a demonstrable risk analysis process and risk management program. Risk analysis is the process whereby security/control measures are selected by balancing their costs against the losses that would be expected if these measures were not in place. It provides a baseline for implementing an effective security plan that protects Agency assets against various threats. (Benson) Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and then maintaining those accepted levels. The HIPAA Security Rule requires both risk analysis and management. The documentation produced by the analysis should also support the decisions the Agency makes as to how they implement the addressable specifications in the Security Rule.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A repeatable methodology is essential for effective risk analysis and management. Tools are an important part. There are several commercial tools that support risk management but many, such as Riskwatch, are very expensive and not within the scope of any proposed Agency budget. As an alternative, I suggested the use of OCTAVE^{sm}, which represents a self-directed approach to risk analysis and whose outcomes support the establishment of on-going risk management.

Besides providing clear, well-structured documentation guidelines, the OCTAVE^{sm} approach was extremely attractive on several other counts. It was:

- Affordable, making use of existing resources to perform the assessment.
- Consistent with the corporate culture that emphasizes open communications and teamwork.
- Complementary to the HIPAA Security Rule. The OCTAVE^{sm} Catalog of Practices was developed using the proposed HIPAA Security Rule (Alberts and Dorofee 455).
- Customizable to met the needs of the organization

This approach also involved the entire Agency workforce with the immediate benefits of raising security awareness levels and increasing the corporate sense of ownership for security through individual participation in the decision making process.

The OCTAVE^{sm} method is defined by a set of criteria that includes:

- **Principles** defined as "the fundamental concepts driving the nature of the evaluation" (Alberts and Dorofee 18) and which embody the philosophy of the method, such as the concept of self-direction, an aspect very attractive to the Agency.
- **Attributes** defined as "the distinctive qualities, or characteristics, of the evaluation" (Alberts and Dorofee 18) and which are derived directly from the principles.
- **Outputs** defined as "the outcomes that the analysis team must achieve during the evaluation" (Alberts and Dorofee 18). In this case, the individuals comprising the analysis team are also the Agency's Security QM team. One of the main reasons why OCTAVE^{sm} was so attractive to the Agency was the format in which the method documented the outcomes.

Normally, the method is accomplished in three phases. These phases are interrelated and do not have to be accomplished in a linear fashion (Alberts and Dorofee 52). The Agency is currently in Phase One, has delayed Phase Two until next year, and is also addressing some of the elements in Phase Three (i.e., basic planning) concurrently with Phase One.

- **Phase One: Building Asset-Based Threat Profiles** presents the organizational view for the evaluation and will be completed in FY 2003. The Agency has already tailored the processes for this phase, simplifying them to meet the needs

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of their environment. The attributes and outputs of this phase have been incorporated into the entity-wide Security Management Plan, the foundation document for the Agency's Security Management Program.

- **Phase Two**: **Identifying Infrastructure Vulnerabilities** presents the Technical View and will be completed in the next calendar year. The Agency originally considered having an external agency conduct an independent evaluation of their infrastructure. This would have included a vulnerability assessment and/or penetration test and represented a sizeable investment. I recommended the Agency delay this expenditure until they fully completed their organizational assessment. The planning and risk assessment activities from Phase One identified specific vulnerabilities for the Agency that they had the skill and ability to address immediately. They should complete at least one internal technical evaluation and audit for themselves. They also need to be able to commit the resources to resolving issues that the independent evaluation will reveal.
- **Phase Three: Plans and Strategies**, which includes risk mitigation activities, are already being worked on since many of the issues are known. Once Phases One and Two are formally completed, the Agency will revisit these initial efforts to clarify and solidify their risk evaluation. In the meantime, they are continuing to adapt the OCTAVE^{sm} method as both a methodology and a tool to support the planned yearly review and update for their security program.

The outputs from OCTAVE^{sm} will be used for the Agency's approach to risk management, enhancing their ability to:

- Reduce the likelihood of a threat from occurring
- Reduce the impact of a threat if it occurs
- Detect the threat when it occurs
- Recover from the threat when it occurs

This process forms a basis for developing key elements of the security plan, policies and procedures as well as needed upgrades or modifications to the facility or information technology infrastructure.

The Agency added a Phase 4 to their process, entitled Manage and Evaluate, based on the risk management principles outlined in OCTAVE^{sm}. The outputs of Phase Four ensure that security is addressed as part of the strategic and operational planning that the Agency does annually. Again, this shows that the Agency has not only committed to information security but intends to keep it integrated with their business objectives.

The following table illustrates how the Agency has adopted the structure of OCTAVE^{sm} to their needs.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

	Principles	Attributes	Outputs: Phase 1 Organizational View:	Outputs: Phase 2 Technical View	Outputs: Phase 3 Security Strategy and Plans	Outputs: Phase 4 Manage and Evaluate
Organizational & Cultural	Open Communications Global perspective Teamwork	Already contained in organizational and cultural principles of agency management				
	Self-directed	QV team augmented as needed by experts with additional skills	Plan documents Analysis Team Experts to Augment Team Skills			
Risk Evaluation	Defined Process for Evaluation (Process)	Security Management Plan (SMP) establishes: Scope Responsibilities Evaluation Activities Tools Common format for documentation (linked to catalog of practices)	Procedures for performing evaluation activities defined and documented in Security Management Plan			
	Adaptable Measures (Product/Data)	Catalog of Accepted Practices Generic Threat Profiles Catalog of Vulnerabilities	Identify Critical Assets Security Requirements Specific Threats Current Security Practices Organizational Vulnerabilities	Identify Key Components Current Technical Vulnerabilities	Identify Risks to Critical Assets Risk Measures	
	Continuous Process	SMP establishes on-going process Identify Implement Manage P&P's for improvement			Develop Protection Strategy Establish Risk Mitigation Plan	
Risk Management	Forward looking view Focus on critical issues	Strategic and tactical plans Organize and prioritize against Agency and IM/IT plans				Agency Strategic and Operational Plans IM/IT Plan Security Management Plan
	Integrated Management	Agency already has established this practice. Security needs must be integrated with key business objectives in Agency plans				

Table 4: OCTAVE^{sm} as Tailored by the Agency

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Document the program via an entity-wide security management plan. The Agency has documented their program in an entity-wide security plan that contains the following (Garbars 7):

- Security management structure and security responsibilities;
- Security policy, procedures, guides, and standards, including established sanctions for security incidents;
- Security training and awareness program;
- Incident and security advisory handling procedures, formalizing the process for incident reporting, including the mechanisms to respond and investigate security breaches or incidents;
- Compliance reviews and enforcement procedures, including vulnerability scanning and penetration testing; and,
- Reference to other, required plans, whether by direct incorporation or by reference.

The entity-wide security plan cannot be static. It will be reviewed and updated annually along with the Agency's Strategic and Operational Plans, IM/IT plans, facility plans, and contingency/disaster recovery plans. It will reflect recommendations and changes that stem from the security program reviews described below. It will also provide standards for documentation and reflect the document management process used for all critical Agency documents.

Establish routine series of Security Management Program Reviews. These reviews will focus on both compliance and enforcement activities and provide continuous process improvement as regards security. The content of these reviews will be reflected in a standard meeting agenda. This agenda includes:

- Review and updates to risk assessment findings and risk management strategies.
- Compliance reviews to include all aspects of the security program and the system infrastructure, based on inputs from system and network management activities. This review serves as the system security configuration management review board. Inputs for these reviews come from the evaluation and review of policies and procedures, security training and awareness, and system, network, and user management activities. This forum will also review any new business associate agreements that involve electronic information or technology.
- Enforcement review, including any incidents and outcomes, and suggested updates to prevent further incidents or exposure.
- Issues and action tracking.

Step Four: Review Agency Contingency Planning Documents

Business continuity is based on the contingency planning to respond to a system emergency. The plan should include the performance and retention of backups,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

preparing critical facilities that may be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. Disaster recovery is the part of an overall contingency plan that contains a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. An emergency mode operation plan, also part of the contingency plan, enables an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure (Federal Register, vol. 63, no. 155, 43266).

The Agency had an existing plan from the previous Joint Accreditation Commission on Healthcare Organizations (JCAHO) inspection. It was reviewed as part of Phase One of the risk analysis, taking into account a basic criticality review that involved the Agency infrastructure and systems, the physical facilities and site plans, and any current procedures and/or plans that include emergency operations, manual procedures, records retention and recovery, and system and network backup and recovery.

Plan elements that did not exist were developed, such as key activities and workflows for response. The Agency modified their procedures as needed and implemented some basic upgrades to the infrastructure, such a backup system for the EMR. The Agency has committed to test the updated plan annually. This will be a comprehensive test that exercises all components in the plan.

Step Five: Identify Key Security Policies

Policies, including those for security, provide a framework the Agency can use to establish necessary levels of information security and privacy and achieve their desired business objectives.

A policy is a statement of information values, protection responsibilities, and organizational commitment for a system (Federal Register, vol. 63, no. 155, 43267). Within the Agency, as with many entities, a policy is considered a high-level legal interpretation of needs. Policies, therefore, carry legal weight and change slowly, usually with the input of legal counsel. Agency security policies apply across the entire organization, including human resources, information technology, records management, facilities management, various programs, and physical sites. The list of policies that fit these criteria is rather short, although the guidance and procedures generated from each area can be extensive. The Agency selected the following areas in the table below as key to their security practice.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 5: Agency Security Policy Framework

Policy Area / Title	Description/Scope	Practice Guidelines
Compliance with Legal and Policy Requirements	Provide guidelines that outline how and why compliance should be managed.	Compliance with Legal Obligations and Policies Avoid Litigation Vendor Agreements Service Level Agreements Data Sharing and Business Associate Agreements Other Legal Issues Established on sanctions
Documentation Standards	Establish procedures for formal documentation and maintenance of policies, guidance, procedures, and practices	P&P Sources of Authority Management Approval Process Policy Maintenance Processes (Creation, Revision, Retirement)
Audit / Certification	Establish methods to effectively and proactively audit for security related issues and incidents. Audits should provide a logical means to establish entity certification and/or formal accreditation by the appropriate sanctioning bodies.	Role and Responsibilities (Internal/External) Processes and Controls (Preventative, Detection, Corrective) Testing Requirements Areas of Focus include, but are not limited to: • Asset Management • Physical Information, Data, and Documentation • Electronic Information, Data, and Documentation • Acquisition and Outsourcing • Information Systems (Stand-Alone, Workgroup, and Enterprise) • Network Infrastructure and Services • Remote Access (Modems, VPN) • Use of Internet, Intranet, Messaging • Mobile Computing
Security Incident Management	Establish the process for detecting and responding to information security incidents.	Definition of Security Incidents/Breaches Monitoring/Detection of Security Incidents Reporting Information Security Incidents Investigating Information Security Incidents Corrective Actions Other Information Security Incident Issues
Personnel Security	Address personnel issues related to security	Personnel Screening/ Clearance for Workforce Members including Staff, Contractors, Vendors Contractual Terms and Conditions Information Related to Security Retained in HR Record (e.g., receipt of training and security awareness) Handling of Information According to Classification Personnel Information Security Responsibilities Management /Supervision Workforce Voluntary and Involuntary Workforce Termination Disciplinary Actions Related to Security

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Policy Area / Title	Description/Scope	Practice Guidelines
Business Continuity	Develop business continuity and disaster recovery plans and procedures.	Business Continuity Plans and Procedures Testing Revision Procedures Incorporation of Related Plans Disaster Recovery Facility and Site Emergency Mode Operations Information Systems Backup and Recovery
Cyber Crime	Establish proactive approach to the combat of cyber crime	Roles and Responsibilities Determination of Threat/Characteristics Monitoring/Detection Investigation/Response

The Agency has designed their policies to be easily understood and enforceable. They consider guidance as the living representation of a policy. Guidance, together with the policy it stems from, forms the basis for workforce compliance and sanctions. Procedures embody the implementation of policy guidance.

The change management process for these documents still needs to be defined, but the evaluation, review and update processes for policies, guidance, and procedures, however, are intended to be part of the routine Security Management Program Reviews.

The Agency has elected to implement a comprehensive electronic document management process, specifically oriented towards this type of documentation. They have the appropriate information management tools within the Agency, but need to customize them to support this workflow. Role-based access to the information will be provided over the Agency Intranet.

Step Six: Review and Update Business Associate Agreements

The Agency has already reviewed the required contractual terms and conditions with all their business associates to ensure HIPAA privacy compliance. The Agency outsources several key areas of IT including the management of their VPN network, desktop and server support, and the phone switch. The VPN vendor is clearly involved in the transmission of electronic PHI and the other vendors have potential access to electronic PHI. The Agency still needs to determine the terms and conditions required by the Security Rule. They will review these with each of their IT vendors and ensure that all contracts and SLAs include the appropriate security provisions as well as those for privacy.

Step Seven: Security Training and Awareness

Within the Agency, the subject of security training and awareness is closely coupled with that of privacy. Security training is considered to be the basic education of the workforce to ensure the protection of the Agency's PHI (Federal Register, no. 63, no.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

155, 43276). Security awareness re-enforces that education, making security part of the daily work routines.

The Agency customizes all their training and awareness programs to a person's role in the organization, focusing on issues directly related to their particular use of health information and the corresponding responsibilities regarding privacy and security. Over the next six months, the Agency intends to develop a program that incorporates IT skills assessment and training in order to avoid security incidents that are unintentional, largely based on a user's lack of fundamental computer skills. The Agency intends to establish a review process for all security training and awareness activities as part of the Security Management Program Reviews.

Step Eight: Technical Considerations

Technical considerations are vital to the Agency's implementation of information security. The following activities have been identified as being the most immediate for FY 2004. (Note: These activities are covered in WBS 7 through 10, outlined in Table 1.)

- *Completion of Phase Two of the OCTAVE^{sm} method.* This step is needed to truly identify the gaps in the Agency infrastructure, perform a vulnerability assessment, evaluate its outcomes, and prioritize all technical issues.
- *Security requirements.* During the OCTAVE^{sm} Phase One process, the Agency established a security database linking their assets, both organizational and technical, to the requirements of confidentiality, integrity, and availability. These requirements provide a structure for process re-engineering, product evaluation, and testing of changes to the security baseline. The use of this requirements database needs to be integrated into the security management processes for the Agency, including change management and control and testing.
- *Documented security architecture.* The Agency's technical security architecture needs to be stabilized, properly documented, and placed under configuration management. Operational processes, performance parameters and service levels should be part of this baseline. Any standards that the Agency adopts to describe their security architecture, including network and system management tools, should be added to the requirements database as well.
- *Business process re-engineering.* Technical solutions need to be evaluated to see if the same effect may be accomplished by a much simpler workaround or technique to evaluate information.
- *Develop Security Operations Plan.* This plan would identify critical system and network management processes, define the metrics and indicators being used, and outline how monitoring and auditing tools should be used as related to security. It documents the audit criteria (i.e., items to look for and/or track), thresholds for significant events, escalation procedures, management reporting procedures for real, potential, or suspected security incidents. It would provide the practical procedures to maintain and manage security configurations, such as procedures for software and hardware installs, upgrades, updates, fixes, tracking changes relative to the security baseline, and subsequent testing to ensure that

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

system security features of a system are implemented as designed and adequate for the applications environment. It would cover backup and recovery operations and tools as well as inventory management including initial logging and disposition of assets (e.g., hardware, software, media).

- *Total Cost of Ownership.* Not only must the initial price for any commercial products be considered, but the costs of customization, maintenance, administration, and updates (such as for virus protection or intrusion detection systems) must also be factored in to the total cost.

Impacts and Accomplishments

Security involves a myriad of processes overlaid on an entity's existing organizational and technical infrastructure. The impact of this entire process was to integrate security practices into the Agency in an orderly and consistent manner. The major challenge was to define and then establish the business processes related to security. These processes required activities that were not necessarily directly security related, such as improvements related to network and systems management activities.

The first steps in the risk analysis process needed to be organizational in scope and cover the entire enterprise. The first stage of developing the overall security practice for the Agency is complete. The Agency has established the management framework they need, has addressed the major organizational issues, and has a well-defined plan for the next fiscal year that includes concentration on the technical issues. Using the approach in this paper, I was able to help the CIO evaluate various scenarios so that he could justify his security program and budget for the next fiscal year.

The accomplishments resulting from the work effort to date include establishment of:

- A security management program with a supporting suite of plan documents as shown in Figure 2. HIPAA required documents are indicated in yellow.
- Organizational responsibilities. Security responsibilities have been assigned to a CSO. Security teams have been identified along with defined lines of communication for both routine and emergency operations.
- A process for security QM representing all areas within the Agency involved in security. A preliminary set of metrics and indicators have been defined and the review process has been described.
- A document management process for both privacy and security artifacts.
- An Agency directed risk analysis process based on the tailoring of the OCTAVE^{sm} method. The building of a demonstrable risk management program based on the outcomes is also well along.
- Continued commitment to an enterprise security practice by executive management. This effort has resulted in an approved budget that includes a technical risk evaluation by an independent party and the acquisition of enterprise level security administration tools.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This effort has provided the Agency with an enhanced awareness and commitment to electronic information security and has seen them move into a leadership role in the regional healthcare community.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

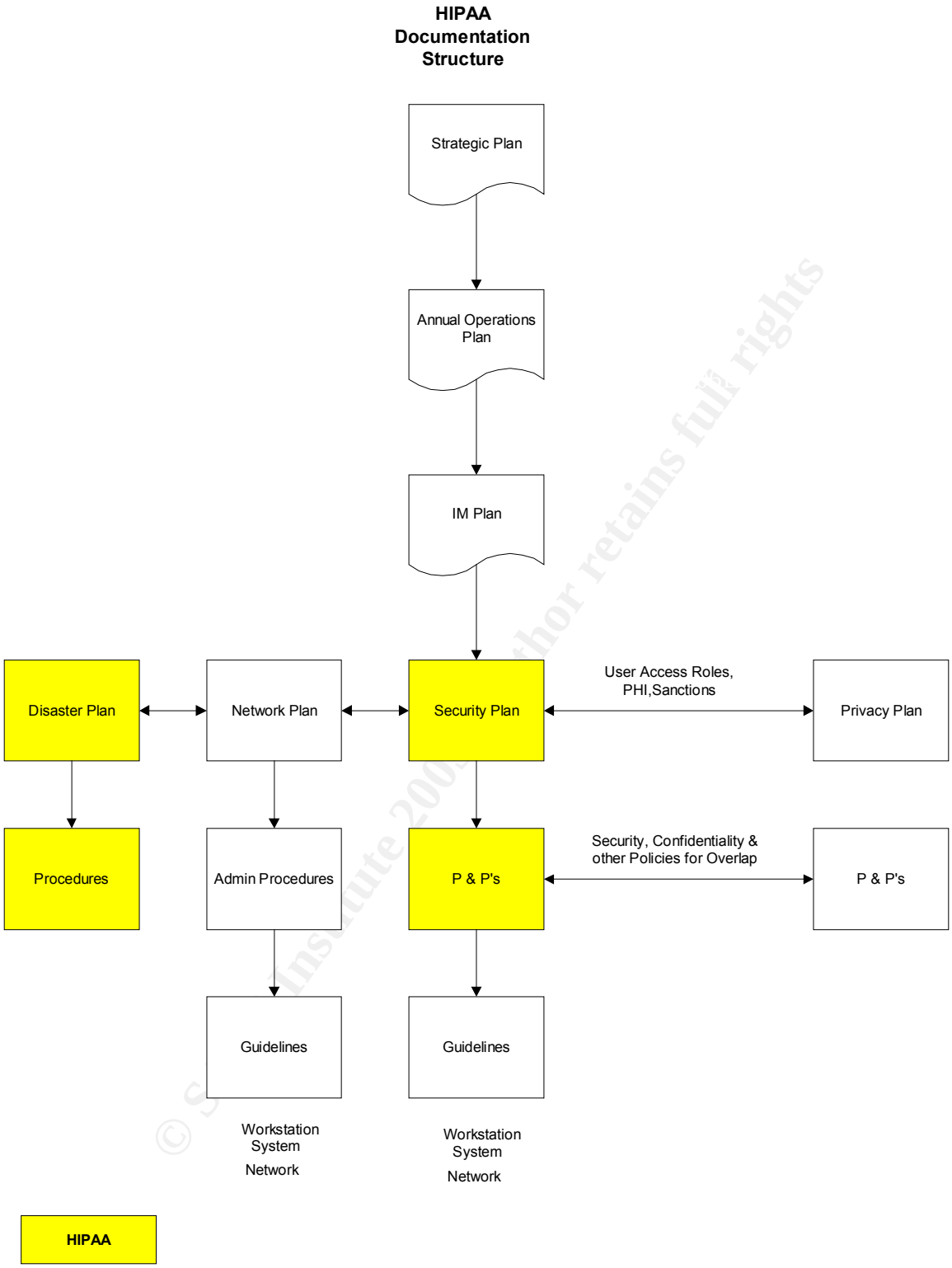

Figure 2: HIPAA Documentation Tree

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The After Snapshot -- Conclusions and Summary

I started this project focused on where I might find gaps in the security profile of a behavioral health agency relative to the final HIPAA Security Rule. What I found was an organization focused on their primary mission of quality care for their juvenile clients, very much concerned about the impacts of HIPAA, and highly dependent on technology and electronic information. I realized that security needed to be an integral part of all organizational processes because of this dependence. Together with the Agency staff, I helped close a large and fundamental vulnerability – lack of security awareness coupled with an ever-increasing dependence on technology.

However, this was only the start. Security had not been considered from the beginning of the Agency's investment in information technology. The Agency needed to 'pause' and design information security back into their whole organization as well as prioritize and correct the multiple technical vulnerabilities that were present in their environment. The situation has caused additional complexities for the IM/T Department as the staff must deal with their daily responsibilities while transitioning to new technologies, tools, and techniques. But, here is where the real success of this project lies. I helped the Agency to establish a framework for sorting through their problems, setting achievable security goals and maintaining control over functional and technical improvements. The Agency now has an on-going cost-effective security program, integrated with current Agency business practices and consistent with their business objectives.

Many security professionals may have focused immediately on establishing a 'defense in depth' technical solution. In my own case, I have always been a 'systems person', where the definition of system follows the convention adopted by HIPAA in §164.304: "A system normally includes hardware, software, information, data, applications, communications, and people" (Federal Register, vol. 68, no. 34, 8340). For scenarios like this case study, one should never lose sight of security in the context of the system -- whether working with the information, the applications, the hardware and software, the networks that transport the data, or ultimately the people who are the users of the technology.

When dealing at the enterprise level within an organization, one oftentimes is faced with an overwhelming number of inter-related and complex security issues. One must take a system view where the 'system' is the entire organization, not just limited to the information systems within it. A methodology, such as presented in this paper, is needed to understand and integrate the technical and functional requirements, the constraints imposed by the environment with the business objectives of the client. This approach allows the development of an overall strategy that addresses a complex scenario in an organized and effective fashion, allowing for a cost effective and implementable security solution, ultimately built upon the materials presented in the Security Essentials course.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. "45 CFR Parts 142. Security and Electronic Signature Standards: Proposed Rule". *Federal Register*, vol. 63. no. 155. (August 12, 1998), 43241-43280.

2. "45 CFR Parts 160. 162, and 164. Health Insurance Reform: Security Standards: Final Rule". *Federal Register*, vol. 68. no. 34. (February 20, 2003), 8334-8381.

3. "45 CFR Parts 160 and 164. Standards for the Privacy of Individual Identifiable Health Information: Final Rule". *Federal Register*, vol. 65. no. 250. (December 28, 2000), 82462-82829.

4. Alberts, Christopher J. and Dorofee, Audrey J. Managing Information Security Risks: The Octave[sm] Approach. Boston: Addison-Wesley Professional, 2002.

5. Benson, Christopher. "Security Planning". Best Practices for Enterprise Security. Microsoft Solutions Framework. Microsoft. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpent/sec1/secplan.asp (May 31, 2003).

6. Garbars, Kurt. "Implementing an Effective IT Security Program." SANS InfoSec Reading Room. Auditing and Assessment. August 28, 2002. 16 pages. SANS. URL: http://www.sans.org/rr/papers/5/80.pdf (May 31, 2003).

7. West-Brown, Moira J.; Stikvoort, Don; Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; and Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. URL: http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html (May 1, 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. 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**