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.

Understanding HIPAA Security Implications Of a Wireless LAN Subsystem Using the ISO/IEC 17799 ISMS Standard

This paper describes the initial development of an Information Security Management System (ISMS) that will address possible regulatory issues of using Wireless LANs in an assisted living / extended care facility (EcFac1). The company has started a major expansion program and will be significantly increasing their reliance on information management systems. The Company does not have a formalized security management system in place and intends to develop one as it rolls out its new information technology (IT) infrastruct...

Copyright SANS Institute

Author Retains Full Rights

AD

Understanding HIPAA Security Implications Of a Wireless LAN Subsystem Using the ISO/IEC 17799 ISMS Standard

By: Frederick Hawkes

G7799 Certification, Version 1.0
New Orleans, LA
June 1, 2004

© SANS Institute 2004, Author retains full rights.

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

Table of Contents

Define the System 4
Project Summary 4
Organization 4
System Description 6
Current Security Structure 8
Plan-Do-Check-Act (PDCA) Process 9
ISMS Project Plan (PDCA … Plan) 10
Project Scope 10
Project Timeline 11
Organizational Structure and Responsibilities 12
Policies, Guidelines, Standards or Procedures Requirements 14
Risk Identification Process 16
Risks to the System 19
Plans for Addressing the Risks 20
Selected ISO17799 Controls 21
ISMS Implementation Plan (PDCA … Do) 23
Overview 23
Creation and Staffing of the Security Management Team 23
Identification and Processing of Applicable Legislation 24
Data Protection and Privacy of Personal Information 25
Information Security Policy Document 25
Information Security Education and Training 26
WLAN Access Control 27
Statements of Applicability 27
ISO 17799 Section 12.1.4 … Data Protection and Privacy of Personal Information 28
ISO 17799 Section 12.1.2 … Intellectual Property Rights 28
ISMS Audit Plan (PDCA … Check) 29
ISO 17799 Section 4.1.1 … Management Information Security Forum 29
ISO 17799 Section 12.1.1 … Identification of Applicable Legislation 30
ISO 17799 Section 12.1.4 … Data Protection and Privacy of Personal Information 31
ISO17799 Section 9.4.3 … User Authentication for External Connections 32
ISO 17799 Section 3.1.1 … Information Security Policy Document 34

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

ISO 17799 Section 6.2.1 … Information Security Education and Training 35
ISMS Maintenance and Improvement (PDCA … Act) 37
On-going Improvement Plans for EcFac's ISMS 37
Regulatory Awareness Program 37
Incident Management 37
Change Management 38
Development of a Business Continuity Planning Process (BCP) 38
Development of a Dedicated Security Awareness Program 38
References 40
Appendix "A" … Proposed Policies 42
Title: Wireless Communications Policy 43
Title: Regulatory Compliance Policy 44
Appendix "B" …HIPAA Security Standards; Final Rule 45
Administrative Safeguards 45
Physical Safeguards 46
Technical Safeguards 46
Appendix "C" Key Security Employee Job Descriptions 47
Chief Security Officer 47
Facilities Security Manager 48

© SANS Institute 2004, Author retains full rights.

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

Define the System

Project Summary

This paper describes the initial development of an Information Security Management System (ISMS) that will address possible regulatory issues of using Wireless LANs in an assisted living / extended care facility (EcFac[1]). The company has started a major expansion program and will be significantly increasing their reliance on information management systems. The Company does not have a formalized security management system in place and intends to develop one as it rolls out its new information technology (IT) infrastructure as a part of its expansion plans.

Due to the nature of their operation (patient healthcare) security is an overdriving force as they develop their new IT capabilities. Current privacy concerns and regulatory affairs such as the Health Insurance Portability and Accountability Act[2] (HIPAA) [1], mandate their attention to security issues required to maintain the safeguarding of patient electronic Protected Health Information (e-PHI). The development of their ISMS under a recognized framework such as ISO 17799 is a natural process to follow.

Organization

EcFac is a private, for-profit assisted living / extended care facility operating a successful and profitable business in Central Florida. With the increasing longevity of American citizens (closely coupled by the "baby boomer" generation nearing retirement), EcFac has projected a significant rise in the need for their services. According to William Novelli in his article "How Aging Boomers Will Impact American Business" of the AARP, "a baby boomer turns 50 every 7.5 seconds" and "the size of the 50+ population will more than double over the next 35 years."[2] EcFac is indeed in a high growth market and plans to position themselves to be a major player.

To position themselves for growth, their management team has developed a phased expansion plan covering the following areas —

- Phase I (In-process … completion expected in Q4/CY2004)
  - Expansion of the existing facility in Central Florida … including the development of a multi-building campus environment on their current property
  - Expansion of their reliance on technology for the monitoring and management of patients, resources and additional items used within the facility including the implementation of a Wireless LAN to improve efficiency and response time to critical events
- Phase II (To begin in early 2005)
  - Development of two additional facilities in the Central Florida area modeled on the success of their current business and the new capabilities that they will be adding as a part of Phase I

[1] EcFac is the pseudonym for a theoretical Extended Care Facility, not an existing organization
[2] Specifically the "Health Insurance Reform: Security Standards" of the Administrative Simplification sub-title of HIPAA [1]

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

  - Expansion of their technology program to include the additional facilities
- Phase III (To begin in mid 2006)
  - Expansion to locations outside of Central Florida (including other states)

One portion of their current business that will be expanding with time and population aging is concerned with patients (also referred to as "residents") that are mentally challenged due to various forms of dementia including Alzheimer's. They want to provide their residents with as much mobility as possible while maintaining their constant oversight and security.

The business is structured into four major line organizations; administrative, information technology, healthcare and operations —

- The Administrative organization includes the senior management of the company including the executive office with the CEO/President and his staff; the Accounting and Finance department, the Marketing and Sales staff, and Human Resources
- The Information Technology Department is responsible for all information processing, data storage and networking assets of the Company.
- The Healthcare organization includes the nursing department, the therapy department, the onsite clinic and the pharmacy
- The Operations organization is responsible for all maintenance services including facility maintenance, grounds maintenance and all equipment maintenance other than IT services related equipment; facility upgrades; site physical security and cafeteria services.

A large percentage of their residents are memory impaired due to Alzheimer's, age related dementia, or other brain related anomalies including stroke and accident trauma. Other residents have physical limitations requiring constant supervision and condition awareness. As a part of its expansion program, EcFac will be installing an extensive wireless LAN (WLAN) that will cover the current facility as well as the Phase I campus expansion. New capabilities being introduced with the WLAN will be highlighted in the System Description section below.

The new CEO brought on board to champion the expansion program has a background in both medical facilities management and the management of a medical equipment manufacturing organizations. His experiences in both arenas have shown him the advantages of working toward industry standards for quality and security. He was exposed to ISO 9000 during his tenure in medical equipment manufacturing and to the need for the adoption of standards for security, especially IT security.

In his last position as Chief Operating Officer for a major hospital where he participated in their HIPAA compliance efforts. He was personally involved with the hospital's HIPAA program because he has always been an advocate for patient privacy and welcomed the oversight brought about by the Privacy and Security rules under HIPAA. While working on the security aspects of the HIPAA program, he became keenly aware of the need to build their security program on a solid framework that encompassed not only the specific requirements of HIPAA, but an overall broad based security program.

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

During the investigative phase of the hospital's HIPAA security effort, the COO was introduced to a new emerging security standard, ISO17799. Having worked under the auspices of ISO9000 in the medical equipment companies, he considered the utilization of an internationally recognized standard as a major plus. In his quest to instill quality as a major part of the expansion program and on-going operations, he has mandated that ISO17799 be used as the structure for their ISMS program. He has been working with his CIO (who is also acting in the position of corporate security officer, CSO) to this end.

The CEO has begun a search for a full-time CSO, a position whose responsibilities will evolve with the expansion program and will include all new facilities as they come on-line. The CSO will be responsible for overseeing both physical and systems/network security programs.

System Description

EcFac currently has an Information Technology (IT) organization headed up by the company's CIO. The facility has a data center, which has more than adequate room for growth to handle the company's expansion program through Phase III. This paper will not focus on the overall data center and related servers and applications, but rather on a portion of the infrastructure, the Wireless LAN (WLAN).

Additional capabilities are being added to the IT structure to increase reliability and employee efficiency that will specifically use the WLAN including —

- Hands-free Voice over IP (VoIP) phones / communicators [3]
- Resident ID bracelets utilizing RFID technology for location and monitoring activities (this relates back to the need to maintain positional awareness of each patient because either of mental or physical limitations)
- Equipment and resource units (e.g. defibrillators, medical carts, etc.) also utilizing RFID tags for location and monitoring[3]
- Staff notebook computers, note pad computers and PDAs
- Other monitoring and management units and applications

The hands-free phones will be utilized by most of the "mobile" staff members as well as the senior staff for instant (and when required, hands-free) communications. The hands-free aspect is extremely important when a worker has both hands in use and cannot "answer" a call or "place" a call in the traditional sense. As an example, if a nurse is supporting a resident and must call for assistance when both or their hands are in use. According to the Vocera Communications paper "HIPAA Data Security and Privacy Standards for Voice Communications Over a Wireless LAN" [4] —

> These mobile healthcare workers can verbally exchange critical information as they deal with patients. They can also connect with vital personnel 'hands-free' since the system employs voice recognition technology. Doctors and nurses can make better and more productive use of their time. The result is improved interaction and efficiency, faster response times, and increased revenues.

[3] A comprehensive overview on the use and capabilities of RFID tags can be found in two recent Scientific American articles [6] and [7]

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

This increase efficiency for medical uses has also been noted in the recent article "VoWi-Fi: Early Adopters Deploy Voice Over Wireless to Gain Mobility and Cost Savings" in Network World [5] “The (St. Agnes Healthcare) study found that each healthcare unit in the 299-bed facility saved an average of 3,400 hours per year, or the equivalent of 1.7 full-time employees.” The system will quickly pay for itself, even including the cost of managing it securely.

Most of the residents in an assisted living facility (ALF) are fairly mobile and therefore able (and encouraged) to move about the facility including the use of outside garden areas adjacent to the facility. Due to this mobility, it is important to be able to locate the residents at all times and to insure that they do not venture into areas where they could be injured (or leave the facility entirely). To assist the staff in locating residents, including keeping them safe, each resident will wear an ID bracelet on their wrist that will include an active RFID transponder. RFID readers will be placed throughout the facility and at all ingress and egress points (positioning sensors at these locations will notify staff members of any attempt by a resident to leave the premises).

RFID transponders will also be placed on all equipment used by the staff in the care and monitoring of the residents. This would include laptop computers and PDAs, defibrillators, EKG units and other similar devices. This would increase efficiency in the facility by eliminating the need to track key resources down if they were misplaced or wandered off (this also reduces theft).

The WLAN will initially use IEEE 802.11b[4] based technology and equipment, and could be upgraded next year to the latest (and highest performance) technology available at that time. The requirements for future upgrades to the WLAN include —

- Support for all current and planned applications and capabilities
- Increased bandwidth and performance
- Increased security

There is no WLAN in place at the current time, so an initial assessment will be performed to determine —

- The applications required
- The specific equipment to be used
- The location of access points (APs)
- Potential sources of interference
- Potential security issues and vulnerabilities

When the existing facility was built, it was extensively wired for network access including the running of CAT-5e cable and video cable throughout the building and the placement of network and video jacks on essentially every wall. In anticipation of the use of wireless access points (APs) and display monitors located high on walls, network connections were also placed in strategic locations close to the ceiling. All of the cable runs terminate at a main distribution panel in the data center communications closet.

[4] Where available, devices supporting IEEE 802.11g will be used to gain advantage of the additional bandwidth (24+Mbps for 802.11g versus 11Mbps for 802.11b) [8]

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

Several intermediate distribution panels with Layer 2 switches are located in utility closets throughout the facility.

Current Security Structure

EcFac places paramount importance on the privacy and security of its residents, and their healthcare records. This was the case before the new CEO was brought on board and is being re-emphasized as a part of the expansion effort underway.

At the present time, system and network security is being managed by the CIO's office and physical security is being handled by the operations department. The CIO has a security architect on staff that holds a GIAC Security Essentials Certification (GSEC) and is a Certified Information Systems Security Professional (CISSP). This individual is responsible for all aspects of IT security including the set-up and management of perimeter security, password generation and management, and the intrusion detection system. She works with other staff members to maintain and execute the company's back-up and data retention system, and she is the chairperson of the incident management team. Over the past several months she has been developing an inventory of documented and implied security policies, procedures and guidelines in place within EcFac. She was hired less than six months ago in anticipation of the expansion program and to assist in the Company's HIPAA security certification efforts.

The operations department has a Security Manager on its staff that holds a Physical Security Professional (PSP) certification from ASIS International (formerly the American Society for Industrial Security). The security manager is responsible for all physical security including the assessment of physical security vulnerabilities, developing physical security policies and procedures and managing the security staff.

The new CEO has started a program for the creation of a security team that would include the CIO, the security individual from the IT department, the (physical) Security Manager, a representative from accounting and the manager of auditing. This team will meet weekly and has the ability to roll other individuals within the company in and out of the team as required. The team has a number of duties within its charter including —

- Planning and executing its HIPAA Security Compliance effort,
- Developing the Information Security Management System (ISMS),
- Creation of the Company's Business Continuity Plan, and
- Development of their formal Incident Response System

As previously noted, the IT security engineer has been developing an inventory of policies and procedures within the organization covering all aspects of security (both documented and implied). The policies and procedures that have been documented exist in a number of different formats and constructions … no standards currently exist in this area. Associated with the lack of uniform policies and procedures covering security, there are also no formal control mechanisms in place for security.

The team has been chartered by the CEO to use ISO17799 as the basis for developing all future security related policies, procedures, processes and guidelines.

The remainder of this paper focuses on the using ISO17799 to develop an ISMS for HIPAA certification and for the WLAN subsystem, including the types of devices being

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

used, specific threats and vulnerabilities of the WLAN as a whole, specific devices connected to that WLAN and the information flowing between the wireless devices and the rest of the IT system over the WLAN.

Plan-Do-Check-Act (PDCA) Process

ISO17799 suggests the use of a process model referred to as the "Plan, Do, Check, and Act" model[5]. The next four sections of this document address each of these four stages of the process model with respect to using ISO17799 to develop those sections of the ISMS important to the installation and operation of a Wireless LAN within the EcFac facility.

A fundamental part of the ISMS planning and development effort is an understanding of the risks involved with becoming HIPAA compliant and the effect of the deployment of a Wireless LAN within the facility on that compliance. The initial risk assessment effort will be conducted by the Security Architect working in conjunction with the other staff members. There are a wide variety of risk assessment techniques available to the Team, both qualitative and quantitative in nature. The Company has decided that the initial risk assessment will be done using a qualitative approach for several reasons —

- The Company is essentially starting from zero on the entire ISMS effort and it will be coming on-line as they are going through and performing their regulatory assessment tasks
- They do not understand everything they need to know about the risk environment and therefore feel that they need to start from a more elementary position and "work their way up"
- They feel that their knowledge of the various quantitative tools is limited and that more time will be required to reach a level of expertise required to use them effectively
- What limited research that they have been able to do, coupled with the composite experience they have, has convinced them that the initial effort using a qualitative approach at this time is far more valuable that waiting to do a more comprehensive quantitative effort after they have either developed the requisite capabilities internally or have hired risk assessment consultants[6]

More detail concerning the risk assessment effort is brought forth in the Risk Identification Process section of this document below.

[5] As noted on HCi's web site, the PDCA model is also referred to as the Deming Cycle or the Shewhart Model. Walter Shewhart worked for Bell Labs as a statistician in the 1930's. W. Edward Deming adopted the model as quality management tool in the 1950's [9].

[6] They have already determined the need to bring a HIPAA Assessment consulting firm on-board and they feel that they will be better prepared after the initial HIPAA Security Assessment to develop and execute a more comprehensive overall security risk assessment program

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

ISMS Project Plan (PDCA … Plan)

Project Scope

The initial objectives of this ISMS development project utilizing ISO17799 include —

(1) Insuring that the new wireless LAN and all applications using the WLAN will be in compliance with the directives of HIPAA concerning the privacy and security of resident (i.e. patient) health and financial data … the major asset is the resident's electronic protected health information (ePHI) and their non-public personal information (NPPI)

(2) Protection of the overall IT infrastructure assets from assault via the Company's WLAN, including possible financial loss and/or loss of corporate reputation

(3) Allow the WLAN security to evolve as the environment for IT security changes including staying ahead of hackers, malware and the possibility of internal fraud and/or abuse

(4) Provide the ability of the security management system to grow as the company proceeds with its phased expansion plans

(5) Finally, beyond the efforts required in item (1) above for HIPAA compliance, insure that all security efforts are developed under the context of "best practices" that may exceed the requirements for HIPAA

Even though a number of factors will contribute to EcFac's ability to achieve the above objectives, having a well thought out and properly designed Information Security Management System will go a long way. It is important to identify the risks to the above objectives and the controls that will be used to alleviate these risks. This is a major tenet of ISO17799.

The "Define the System" section above highlighted the current security baseline —

- There is no formal security policy program
- There are very few security policies are in place
- Overall security in the organization is somewhat distributed with no central oversight … physical security handled by operations, systems and network security is handled by IT, and personnel security is handled by human resources

But some progress has been made —

- The new CEO had a major role in the development of security compliance for his former employer
- A security oversight team has been set up by the Company's senior management committee … one of their primary assignments is the development of an ISMS
- The team will be developing a security program based on ISO 17799
- The full-time position of Chief Security Officer is being set up

The following table relates the primary business objectives of the Company, the risks to those objectives and the controls that will be utilized to managed the associated risks.

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

Business Objective	Risks to Achieve Objective	Controls to Manage Risks
Insuring regulatory compliance	• Uncertainty of applicable regulatory initiatives • The Company does not know what is required to become compliant with the HIPAA security regulation • Improperly trained staff members at all levels	• Determine what regulatory actions under which they will be operating • Performing a compliance assessment • Awareness training
Maintaining the security and confidentiality of residents' private information	• Unauthorized access to confidential information (corporate and resident) resulting in alteration, theft or loss of private data	• Becoming compliant with required governmental regulations (e.g. HIPAA) • Utilizing all available security capabilities of the new WLAN technology
Protecting the IT infrastructure from WLAN vulnerabilities	• Improper access to corporate assets through unauthorized use of the WLAN resulting in loss of corporate data • Disruption of IT services	• Utilizing all available security capabilities of the new WLAN technology • Conducting WLAN audits (see [10])
Increasing efficiency through use of WLANs	• Unauthorized usage of WLAN resulting in loss of available bandwidth • Disruption of WLAN-based services	• Utilizing all available security capabilities of the new WLAN technology • Conducting WLAN audits
Developing security framework for expansion efforts	• Failure to build and use a comprehensive framework for the base ISMS that will grow as the expansion progresses	• Developing a thorough knowledge of information security management systems • Implementing a comprehensive ISMS

Table 1

Project Timeline

All work on this program will be monitored using Microsoft Project. The following is an overview of the major tasks of this project —

- Creation of a Security Management Team
- Determination of regulatory compliance requirements
- Development of an Information Security Management System (starting initially with the WLAN) including the adoption and use of job descriptions
- Design and implementation of the WLAN including applications using the WLAN and all security measures to maintain the integrity of the overall IT infrastructure

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

- Hiring a HIPAA Security Assessment consultant
- Providing security awareness training for all employees

The above major tasks have been broken out further and are listed in the following Project Plan. Most of these tasks will be completed as a part of the "Phase I" effort highlighted in the Organization subsection above. That phase was due to be completed by the end of 2004, and the following schedule shows a completion date at the end of October of 2004.

	Task	*Duration*	*Start*	*Complete*	*Predecessor*
1					
2	**Determination of Regulatory Compliance Requirements**	**20 days**	**05/26/2004**	**06/22/2004**	
3	Develop List of Regulatory Exposures	5 days	05/26/2004	06/01/2004	
4	Determine Regulations Applicable to EcFac	5 days	06/02/2004	06/08/2004	3
5	Obtain Copies of Applicable Regulations	5 days	06/09/2004	06/15/2004	4
6	Determine Compliance Deadlines	2 days	06/16/2004	06/17/2004	5
7	Prepare Compliance Checklists	3 days	06/18/2004	06/22/2004	6
8					
9	**Develop Information Security Management System**	**109 days**	**05/26/2004**	**10/25/2004**	
10	**"Plan" Phase**	**27 days**	**05/26/2004**	**07/01/2004**	
11	Determine Business Objectives	2 days	05/26/2004	05/27/2004	
12	Prepare Management Committee Presentation	2 days	05/28/2004	05/31/2004	11
13	**Creation of a Security Management Team**	**10 days**	**06/01/2004**	**06/14/2004**	
14	Management Committee Sign-off	2 days	06/01/2004	06/02/2004	12
15	Obtain Team Member Commitments	2 days	06/03/2004	06/04/2004	14
16	Hold Initial Team Meeting	1 day	06/07/2004	06/07/2004	15
17	Prepare Team Charter and Mission Statement	4 days	06/08/2004	06/11/2004	16
18	Prepare Initial Task List	3 days	06/08/2004	06/10/2004	16
19	Assign Responsibilities	2 days	06/11/2004	06/14/2004	18
20	Identify Critical Assets	3 days	06/15/2004	06/17/2004	19
21	Identify Existing Policies, Procedures, Guidelines, and Other Pertinent Documents	3 days	06/15/2004	06/17/2004	19
22	Identify Risks	5 days	06/18/2004	06/24/2004	21
23	Prepare Risk Mitigation Plans	5 days	06/25/2004	07/01/2004	22
24	**"Do" Phase**	**8 days**	**07/02/2004**	**07/13/2004**	
25	Determine Problems with Existing Security System	3 days	07/02/2004	07/06/2004	23
26	Develop Action Plan to Resolve Issues	5 days	07/07/2004	07/13/2004	25
27	**"Check" Phase**	**14 days**	**07/14/2004**	**08/02/2004**	
28	Develop Audit Checklist	5 days	07/14/2004	07/20/2004	26
29	Determine Controls for Audit	4 days	07/21/2004	07/26/2004	28
30	Develop Test Plan	5 days	07/27/2004	08/02/2004	29
31	**"Act" Phase**	**60 days**	**08/03/2004**	**10/25/2004**	30
32	Design and implementation of the WLAN	20 days	07/14/2004	08/10/2004	26
33	Perform a HIPAA Security Assessment	20 days	07/02/2004	07/29/2004	7, 23
34	Providing security awareness training for all employees	20 days	07/30/2004	08/26/2004	33

Table 2

Organizational Structure and Responsibilities

EcFac is organized as depicted in the following organizational chart. The security related responsibilities for key employees are delineated after the chart.

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

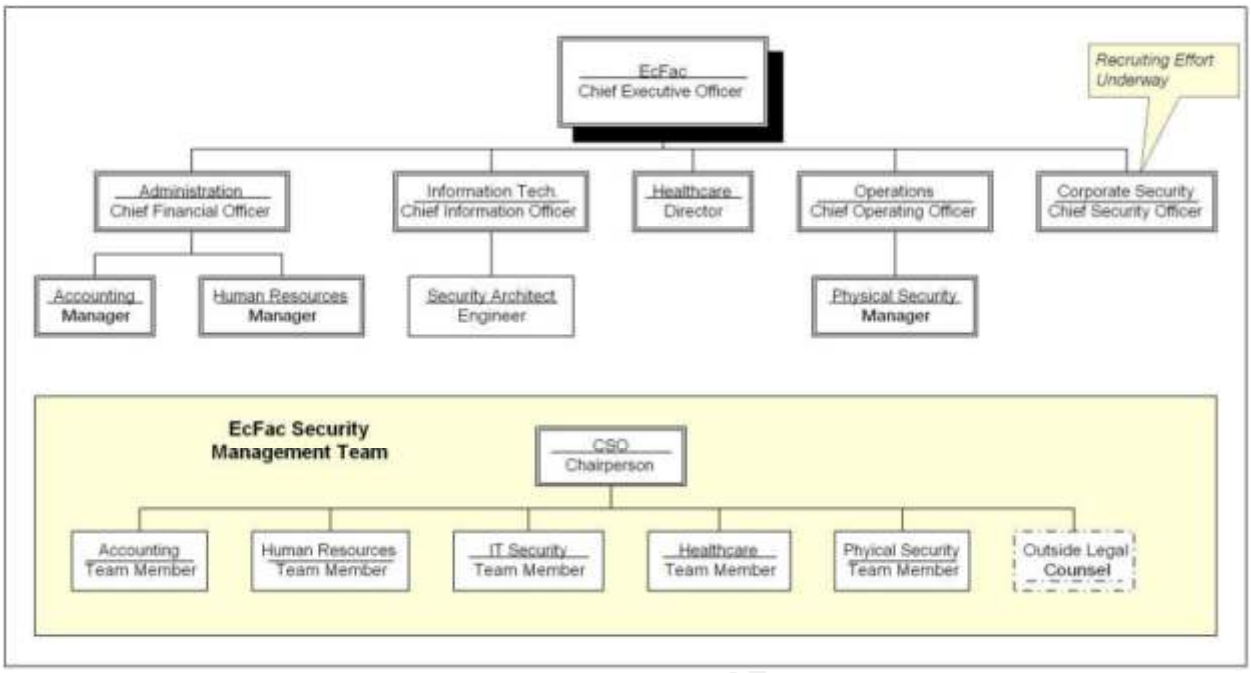

Figure 1 – Organization Chart

- Chief Executive Officer (CEO) – The CEO is responsible for the operation, management and execution-to-plan for the entire company (EcFac). The position reports to the Company's Board of Directors. The CEO must be apprised of all security plans and policies, as well as all security related breaches and other incidents. The CEO will have final approval authority of all security related purchases and new employee hires.
- Chief Financial Officer (CFO) – The CFO will be responsible for insuring that all security related expenditures are made in compliance to the Company's Strategic and Annual Operating Plans. The CFO's staff member participating on the Security Management Team (the accounting team representative) will provide the CFO with all financial material on security related projects in order for the CFO insure the stated compliance.
- Chief Information Officer (CFO) – The CIO is operating as the acting CSO until a full-time CSO can be brought on board. During this interim period, the CIO will have the additional responsibilities outlined for the CSO (see below and in Appendix "C").
- Healthcare Director – The Healthcare Director will be a permanent member of the Security Management Team and will provide inputs to the team on what constitutes protected health information used within the IT infrastructure (ePHI).
- Chief Operating Officer (COO) – The COO will act in a manner analogous to the CFO except concerning himself with managing the "physical aspects" of security. The Manager of Physical Security reports to the COO and provides the COO with reports on the status of physical security for all present and planned sites for the Company. The COO, working with the CFO, will be responsible for contracting with outside companies providing security related services to the Company including the following —

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

  - Construction of physical security elements (e.g. fire control systems, physical intrusion detection systems, physical surveillance devices (e.g. cameras), entry and exit control systems, fences, etc.
  - Contracting with outside security guard firms
  - Contracting with off-site storage companies including storage of system back-up media
  - Oversight of the removal and destruction of confidential material when mandated by the ISMS

- Chief Security Officer (CSO) – The CSO will hold the primary responsibility for all security within EcFac. It is an "umbrella" position reporting directly to the CEO. The full job description for the CSO can be found in Appendix "C" and was developed from a generic position description obtained from CSO Online [11].
- Manager of Physical Security – The Manager of Physical Security will hold the primary responsibility for all physical security within EcFac. This position reports directly to the COO and has a dotted line report to the CSO. The full job description for the manager can be found in Appendix "C" and was developed from a generic position description obtained from the University of New Mexico [12].
- Security Architect (SA) – The SA will be responsible for the overall architecture of the IT infrastructure including the WLAN. Where the SA does not have the expertise or "bandwidth", she will work with the CIO (with a dotted line report to the CSO) to assign and utilize other IT staff members in their specific areas of responsibility and expertise (e.g. using network engineers to set up, monitor and manage the security aspects of the company's networks including the WLAN).
- Accounting Team Representative (ATR) – The Accounting Team Representative will be responsible for all of the "accounting and finance" aspects of security program undertaken by the Security Management Team. The ATR will develop financial analyses for projects, determination of budgeting sources, development of financial alternatives and financial projections for project plans. This information will be reviewed by the CSO and sent to the COO, the CIO or CFO (as required) and then the CEO for sign-off.
- Human Resources Representative – The HR representative will support the Team in areas such as personnel security issues and awareness training.
- Security Management Team – All of the above individuals will be full-time or interim (as needed) members of the Security Management Team. The Team has been charged with the overall security of the IT infrastructure and all physical security requirements related to securing it. The Team is also responsible for seeing that the ISMS is generated and maintained.

Policies, Guidelines, Standards or Procedures Requirements

Wireless Communications Policy

The following policy is a modification of the one developed by Brian Corcoran as a part of the SANS Institute Security Policy Project [13]. Again, the portion of EcFac's IT infrastructure being examined as a part of this paper is their new wireless LAN with the

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

applications and components outlined in the System Description section above, so security of the WLAN is of paramount importance to the Security Team.

1.0 Purpose
This policy prohibits access to <Company Name> networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by InfoSec are approved for connectivity to <Company Name>'s networks.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of <Company Name>'s internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to <Company Name>'s networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards
All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by InfoSec. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with InfoSec

3.2 Approved Technology
All wireless LAN access must use corporate-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication
All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.4 Setting the SSID
The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

3.5 Testing the Wireless LAN
The integrity of the WLAN will be tested on a regular basis using the most current version of the WLAN Vulnerability Assessment Procedure <Document Number>

4.0 Responsible Organization
The Network Engineering Team within the Information Technology Department will be responsible for the management and execution of this policy.

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

6.0 Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

7.0 Revision History
July 10, 2003, Section 3.4 Added
July 6, 2003, expanded to support CDI Initiative, Stephen Northcutt
May 20, 2004, added Section 5.0 "Responsible Organization"; changed subsequent section numbers

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

This policy is structured in the manner that most, if not all, of EcFac's security policies will be prepared, and therefore represents the template for all other security policies. All security policies will consist of the same major sections —

- The purpose of the policy
- Its scope … what components of the infrastructure are covered by it
- The policy statements themselves including references to related procedures and guidelines
- Who is responsible for enforcing the policy
- How the policy will be enforced
- References to the policy including definitions
- Revision history

Risk Identification Process

For this project it was decided that the Cause Consequence Analysis (CCA) method would be used for analyzing the risks [14]. CCA is a tree-based approach to risk analysis using two types of trees —

- Fault Trees
- Event Trees

Both types of trees are used for identifying faults. The Fault Tree is used to determine the underlying causes of the faults, whereas the Event Tree is used to identify the consequences of the faults.

The following Fault Tree depicts several possible underlying causes in the possible failure to achieve compliance to the HIPAA Security Rule. Specifically, an organization might fall short in their efforts to achieve HIPAA Security Compliance by failing to correctly implement any one of the eighteen "security standards" specified in the Security Rule.

We can look at the Security Awareness and Training standard, section 164.308(a)(5), of the HIPAA Security Rule which is comprised of four implementation specifications —

- Security Reminders – HIPAA Privacy Rule Section 164.308(a)(5)(ii)(A)
- Protection from Malicious Software – HIPAA Privacy Rule Section 164.308(a)(5)(ii)(B)
- Log-in Monitoring – HIPAA Privacy Rule Section 164.308(a)(5)(ii)(C)
- Password Management – HIPAA Privacy Rule Section 164.308(a)(5)(ii)(D)

Failure to implement any one of these four specifications would result in a failure to meet the Security and Awareness Training Standard under HIPAA. The Fault Tree shows that two of the specifications have not been adhered to … Security Reminders and Password Management. Again, a failure to meet any one of the eighteen standards by failing any of the 42 underlying specifications could prevent compliance.

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

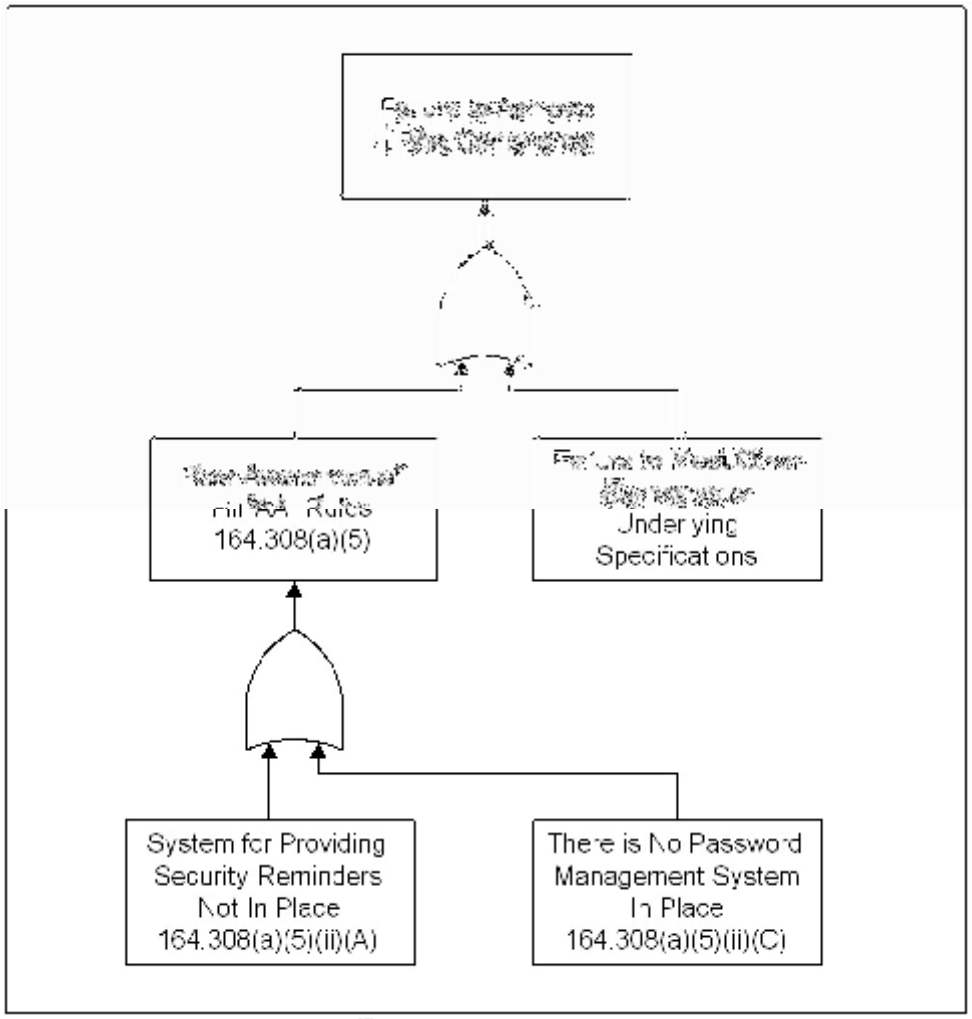

Figure 2 – HIPAA Compliance Faults Tree

The next figure depicts the fault of the "loss of patient data". The tree depicts three different possible underlying reasons that could result in patient data loss —

- Failure to understand the proper methods for using the WLAN or any of the applications that use the WLAN (e.g. failure of a user to change the default password on their PDA)
- The willful theft of patient data by someone on the staff
- The undetected, unauthorized access of patient data through the WLAN (e.g. possibly by a person located outside of the facility using a laptop and determining that the WEP encryption system used on the WLAN has not been enabled

The latter of these three reasons for the potential loss of patient data is highlighted in the figure. In this case, the loss occurred because a component of the WLAN (e.g. an Access Point) did not have its WEP security properly set up, an intruder was able to gain access to the Access Point because of the lapse in security, ***and*** finally, the intruder's presence was not detected by the network Intrusion Detection System.

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

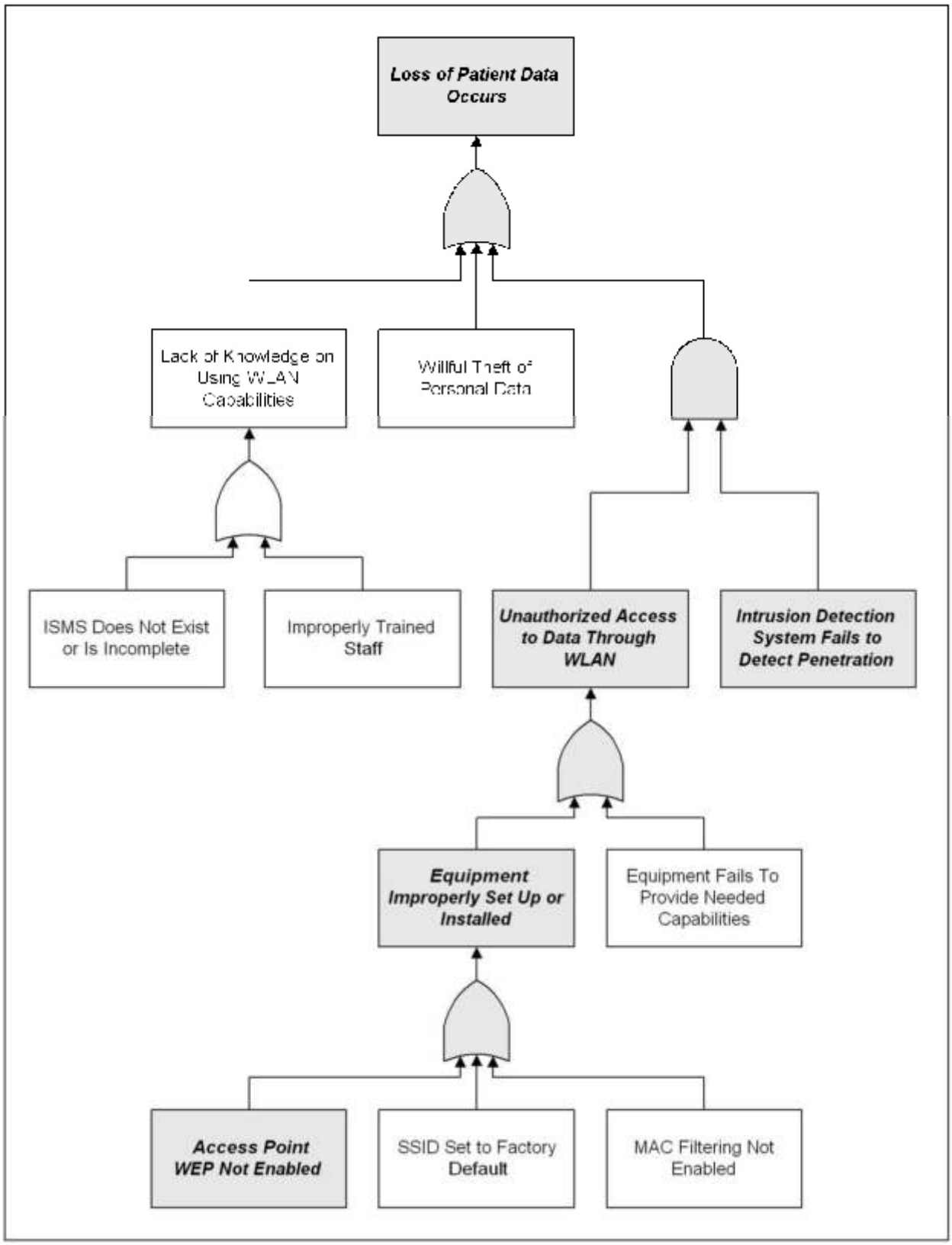

Figure 3 – Loss of Patient Data Fault Tree

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

The above two figures are examples of using fault trees for risk assessment. Cause Consequence Analysis (CCA) also uses the concept of an event tree. The event tree starts from the perspective of an event occurring and examines the effect on that event by examining the affect of mitigating events occurring. In the following figure, we started with an intruder making an attempt to improperly obtain patient data. We then look at two controls that could prevent the intrusion from occurring —

- WLAN security is properly enabled (i.e. SSID, WEP and MAC Filtering [15]), and
- An Intrusion Detection System (IDS) is properly installed and working

If the WLAN security blocks the intruder, or if the IDS system detects the intruder (and a person or system element prevents further intrusion), then no data will be lost. This is depicted on the top line of the right most column (the outcome column) of the figure. In a similar fashion, if the WLAN security works and the IDS would have failed to detect the intrusion, or if the WLAN security failed but the IDS system succeeded, then data would not have been lost in either case (the second and third rows in the outcome column).

On the other hand, if the intruder were able to get past the WLAN security and the IDS failed to detect the intruder, then the loss of data could indeed occur (the last row in the outcome column).

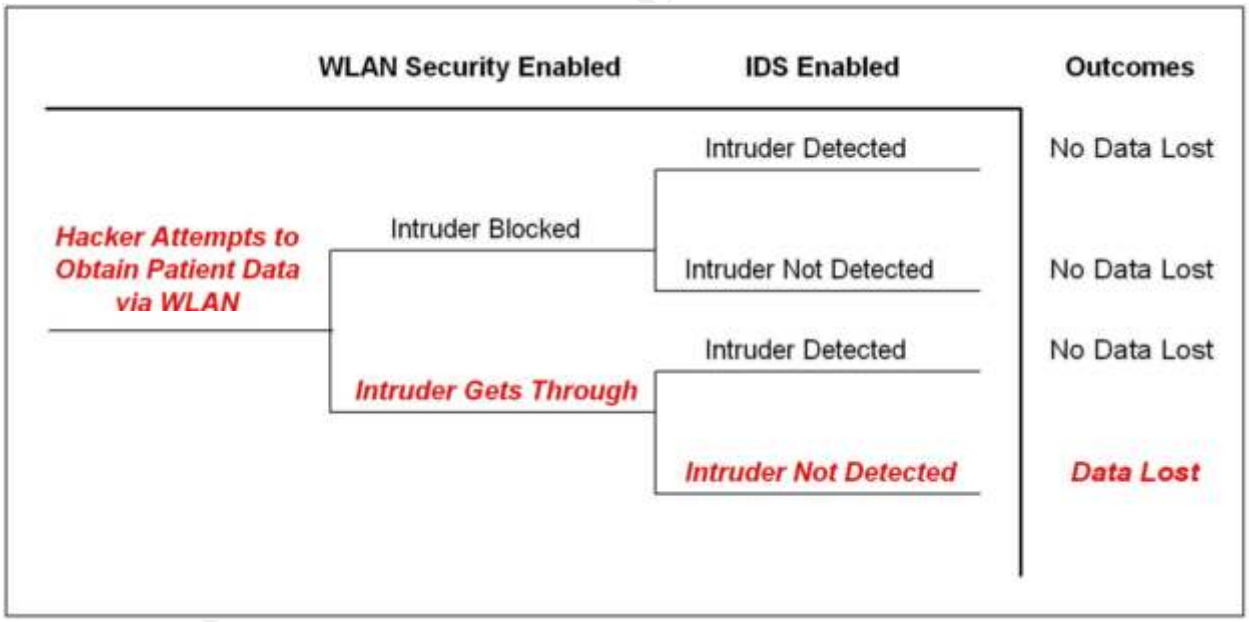

Figure 4 – WLAN Intrusion Event Tree

Risks to the System

As the Company examined its findings from the Risk Assessment, the fundamental questions as to the initial thrust were again raised —

- What actions are required to work toward compliance under HIPAA?
- What were the implications with respect to the Wireless LAN?

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

- What other regulatory actions should be investigated?

The Team went back to the senior staff with their initial findings. At that meeting, the decision was made to focus on the first two. Looking at these two areas of immediacy, the following risks were selected as the highest priority —

1. The Company does not fully understand what it has to do to become compliant with the HIPAA security regulation or the costs of failing to do so
2. The potential exists for unauthorized access to confidential information (corporate and resident) resulting in alteration, theft or loss of Company or private data
3. The possibility exists for improper use of corporate assets through unauthorized access of the WLAN
4. There is a significant lack of knowledge throughout the organization about HIPAA, and about the set up and use of the WLAN
5. Overall security in the organization is somewhat distributed with no central oversight
6. There are very few security policies are in place

Plans for Addressing the Risks

In order to address these risks, and minimize the exposure to EcFac, a set of controls must be acquired or developed to insure the Company's compliance under HIPAA and the security of the WLAN to that end. The following controls will address the above risks as number —

1. Prepare a formal plan to address the issue of compliance with HIPAA and any other local, state or federal regulations that the Company will be subject to. The plan will include a formal gap assessment supported by outside expertise where necessary.
2. Develop a system to protect patient data and limit access to that data to only those individuals and applications that must access the data over the WLAN in the normal course of business.
3. Control #2 above needs to also insure that the WLAN cannot be used to access other portions of the Company's IT infrastructure via the WLAN.
4. Create a training and awareness program to educate employees, consultants and business partners on the privacy and security requirements of HIPAA and how the WLAN folds into those requirements. The training system must be able to show who received what training, when, and what their retention levels were.
5. The Company has decided to create a Security Management Team (Security Forum) to provide a centralized security management capability.
6. Develop a comprehensive set of policies that addresses all of the above risks, how to deal with them and who would be responsible for those actions. The policies should follow the sample policy depicted in the Policies, Guidelines, Standards or Procedures Requirements section above.

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

Selected ISO17799 Controls

It was determined that the following ISO17799 controls would apply to this program —

- ISO 17799 Section 3.1.1 … Information Security Policy Document(s) – This control covers the creation of policy documents that are relevant to the project being covered by this effort. In this case we are concerned with the protection of patient information (as it pertains to HIPAA … at least initially), the development of regulatory compliance security efforts (again with the initial focus on HIPAA), and with the viability of the WLAN that will be used in this facility (and others as expansion plans move forward).
- ISO 17799 Section 4.1.1 … Management Information Security Forum – The Company's senior management has determined that the creation of a Security Forum (referred to as the Security Management Team) will be formed in the Company. This team (working under the direction of senior management) will establish the Company's security policy; insure that the policy is known to everyone within the company; and work to insure that the controls are in place to implement the policy. The Team will be represented by all major departments within the Company.
- ISO 17799 Section 6.2.1 … Information Security Education and Training – As noted in the preceding control statement concerning the Security Forum, the Team will be responsible to see that everyone within the Company understands their duties and responsibilities under the Company's security umbrella. This will be handled through a formal security awareness and training effort. Section 6.2.1 of ISO17799 states that "All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures." Because the cost of a security failure could be high in the Company's business, everyone within the organization must take security seriously, and education supported by testing is essential.
- ISO17799 Section 9.4.3 … User Authentication for External Connections – Wireless LAN technology includes a number of built in security mechanisms. In addition, WLAN technology including security capabilities is constantly improving. The need for one or more controls to address the current security capabilities as well as how security of WLANs is evolving must be put in place. Section 9.4.3 covers this control.
- ISO 17799 Section 12.1.1 … Identification of Applicable Legislation – The senior management team is aware that they are covered under HIPAA because they deal with patient data which is protected under HIPAA. They are concerned about other regulatory initiatives that they might be subject to such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley, and others. Section 12.1.2 of ISO17799 states that "All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system." To this end, the Team will work to insure that it identifies local, state and federal regulations that they will be subject to, and the effect that these initiatives will have on the Company's IT systems (including the WLAN).

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

- ISO 17799 Section 12.1.4 … Data Protection and Privacy of Personal Information – As noted above, HIPAA is extremely specific in the protection of patient privacy and of their medical data. Section 12.1.4 of ISO17799 specifically states that "Compliance with data protection legislation requires appropriate management structure and control." This is also the very essence of the HIPAA Privacy Rule coupled with the HIPAA Security Rule … patient electronic Protected Health Information (e-PHI) must be kept private and secure.

© SANS Institute 2004, Author retains full rights.

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

ISMS Implementation Plan (PDCA … Do)

Overview

The following sections identify the HIPAA certification and WLAN pre-implementation tasks to be accomplished prior to setting up the WLAN itself. The tasks are presented in the order in which they are being tackled (as outlined in the WLAN ISMS Project Plan).

Creation and Staffing of the Security Management Team

Problem Description – Even though EcFac has a number of staff members with security experience, senior management feels that additional expertise will be required. As noted in the Current Security Structure section, the management committee has approved the CEO's proposal to build a multi-departmental security team. Two of the representatives on the team will be the current Security Manager from the Operations Department, who is currently responsible for physical security, and the IT department's Security Engineer. It was also noted that the CEO is in the process of recruiting a Chief Security Officer (CSO) who will act as the Chairperson for the Security Team. Until that time, the Company's CIO will act in that capacity.

The Team will be expanded to include a representative from the Healthcare Department and a representative from the Finance Department. The responsibilities of these individuals were laid out in the Organizational Structure subsection of the Project Plan section of this document.

Action Plan – The CEO began this process by placing a proposal before the Company's senior management committee. The effort has been discussed and is being tracked in the weekly senior staff meeting. The responsibility of the Team will be consistent with the guidelines laid out in section 4.1.1 of ISO17799 [16], which specifically states that the Security Team (Forum) will —

- Review and approve information security policy and overall responsibilities;
- Monitor significant changes in the exposure of information assets to major threats;
- Review and monitor information security incidents;
- Approve major initiatives to enhance information security

Action Steps –

1. Obtain corporate approval of a Security Management Team (approved at the senior staff level)
2. Set aside time on a weekly basis from the Team members' principal responsibility to participate in the team
3. Conduct weekly Team meetings unless required more frequently due to deadlines or incidents occurring
4. Have the Team draft a formal charter and submit to senior management for approval

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

5. Establish a set of "work standards" for the Team to include regular Team activities, formats for work documents including policies and procedures, recording of meeting minutes, etc. Where required (as determined by the Team) see that all resulting efforts are reviewed with, and where necessary, approved by senior management
6. Develop committees (using additional personnel as required and approved by senior management) to be responsible for specific security initiatives formed by the Team (e.g. periodic wireless vulnerability assessments, regulatory review, security awareness training, etc.)

Identification and Processing of Applicable Legislation

Problem Description – Because the Company's activity involves obtaining, developing, using and storage of personal information of the residents (e.g. healthcare data), the senior staff is very aware of the need to understand and comply with local, state and federal regulations regarding such information. The need for compliance with the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act (HIPAA) is well know because the staff members (especially the healthcare staff) is constantly exposed to and processes healthcare data.

In addition to HIPAA, other regulations must eventually be examined for applicability to EcFac. The Gramm-Leach-Bliley Act (GLBA) is one such regulation.

Action Plan – The effort will begin with an analysis of HIPAA to determine what is specifically required with respect to Information Systems security of residents' healthcare information. Following the HIPAA effort, examine GLBA and other possible regulatory requirements. It is well understood that HIPAA is very policy and process driven, so an inventory of all systems, networks, applications and security policies is required. The actions taken here will be consistent with section 12.1.1 "Identification of applicable legislation" of ISO17799.

Action Steps –

1. Obtain copies of the two key regulations … HIPAA and GLBA
2. Obtain copies of all existing policies, procedures, processes and guidelines that have anything to do with Information Security
3. Develop the inventory of systems, networks and applications that will be processing, storing or manipulation resident information in any way
4. Work with SANS, CMS (the Center for Medicare and Medicaid Services), and trade organizations such as the Florida Assisted Living Association (FALA) and the Assisted Living Federation of America (ALFA) to obtain the names of firms that have HIPAA assessment experience (specifically in the support of assisted living facilities).
5. Determine the cost benefit for using such expertise versus developing the expertise and doing the assessment internally
6. Develop a HIPAA compliance plan for Security and Privacy. This Plan will include conformance to section 12.1.1 of ISO17799.

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

7. Develop a Policy for the on-going effort to maintain compliance with all applicable local, state and federal regulations such as HIPAA. This policy will require the review and approval of the Company's senior staff as well as their outside legal counsel.

Data Protection and Privacy of Personal Information

Problem Description – HIPAA is very explicit concerning the privacy and security of an individual's health data (referred to as Protected Health Information, PHI) and its storage and usage in automated systems as electronic PHI or e-PHI. One of the control elements within ISO17799 (section 12.1.4 "Data protection and privacy of personal information") indicates that a properly constructed ISMS would include provisions covering personal information privacy, and hence its security.

Action Plan – All applications and processes utilizing the WLAN will have to be examined to determine what personal information (e.g. healthcare data) is used by them and how it can be kept confidential. A set of policies covering this fact will have to be developed and implemented by the Security Team.

Action Steps –

1. Develop a list of all applications and processes that will comprise or utilize the Company's Wireless LAN.
2. Examine each item from step one to determine what private information will be carried by the WLAN.
3. Develop a list of all devices that will be used to comprise the WLAN and hold the applications running over the WLAN including access points (APs), health monitoring devices (e.g. ambulatory cardiac monitors), data processing devices such as tablet PCs and PDAs, and patient "electronic charts".
4. Determine what security requirements are mandated by the above identified regulations (e.g. HIPAA has standards and specifications concerning the transmission of data that may contain ePHI). The controls of ISO17799 meet or exceed the requirements of HIPAA (see page 20 of [17]) in this area.
5. Develop a policy covering the security requirements HIPAA as they relate to the transmission and storage of ePHI.
6. Using the policy in step 5 as a basis, develop an implementation plan (including management and monitoring actions) that uses the security mechanisms utilized in (or could be added to) the network and system devices used within the WLAN.

Information Security Policy Document

Problem Description – Several of the above action efforts specifically point out the need for documented policies. Further, section 162.308(a)(1)(i) "Standard: Security management process" of the Final HIPAA Security regulation specifically states that a covered entity must "Implement policies and procedures to prevent, detect, contain, and correct security violations", i.e. it must have an Information Security Management System, ISMS, in place as a part of compliance.

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

Action Plan – The Security Management Team will be charged with the responsibility to develop a complete ISMS that will place it in compliance with the Final HIPAA Security Regulation. This is consistent with section 3.1.1 "Information security policy document" of ISO17799.

Action Steps –

1. Develop a detailed list of policy requirements that should be associated with all of the three required sets of safeguards (administrative, physical and technical) of the Final HIPAA Security Regulation (this list has been included in this document as Appendix "B").
2. If an independent firm will be used to perform a HIPAA Security Assessment, work with that firm to determine what policies may already be in place and whether those policies will meet HIPAA guidelines.
3. Prioritize the list of required policies.
4. Using the Policy Template developed in Step 5 of the "Creation and Staffing of the Security Management Team" Action Plan, develop the required security policies per the above prioritized list.
5. Obtain required reviews and approvals for each policy developed per section 3.1.2 "Review and evaluation" of ISO17799 and place them under a Change Control system.
6. Distribute all developed policies to individuals who have the responsibility to execute and manage them (as delineated in section 5.0 of each policy).

Information Security Education and Training

Problem Description – Section 6.2.1 "Information security education and evaluation" of ISO17799, as well as Section 164.308(a)(5) "Security Awareness and Training" of the HIPAA Final Security Regulation, specifically designate the need for "appropriate training and regular updates" in policies and procedures.

Action Plan – In keeping with both ISO17799 and HIPAA regulations, all employees must be made aware of the need for security and their role therein. The information that all employees, contractors and business associates must be aware of under security must be turned into formal training material and delivered to those departments and individuals under a "need to know" doctrine.

Action Steps –

1. Using the policies developed as a part of the above Information Security Policy Document effort; develop a program to create the required training and awareness curriculum.
2. Determine the appropriate media for delivering the awareness and task training.
3. Develop the actual training material and comprehension/retention quizzes.
4. Work with Human Resources to create a system for tracking the delivery of required training on an entity-by-entity (e.g. individual) basis.

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

5. Deliver the actual training. Maintain records of who took the training, when they took it and the course revision level.
6. Quiz all trainees to determine their level of comprehension and retention.

WLAN Access Control

Problem Description – The planned use of a WLAN within the facility is intended to provide added security for the patients, timely location of people and assets, and increases in overall staff efficiency. The problem with using WLANs is their susceptibility to external intrusion and the resulting vulnerability to the Company's IT infrastructure and data contained within the system (especially protected health information). Section 9.4.3 of ISO17799 emphasizes the need for authentication of individuals and devices to internal networks.

Action Plan – Develop and implement the proper mechanisms for preventing unauthorized access to the IT infrastructure through the WLAN. This will include the use of WLAN security mechanisms built into the devices that will comprise the WLAN, and the need to keep informed as to new security features and technologies as they become available.

Action Steps –

1. Determine the architecture for the WLAN (including all devices making up the WLAN, all devices legally attaching to the WLAN, and all application systems that will have access to the WLAN and transfer private information over the WLAN).
2. Insure that all available security mechanisms for the resources identified in step one are fully set up and operational when the WLAN goes on-line.
3. Insure that all security mechanisms previously identified are interoperable.
4. Develop capabilities to periodically test the WLAN to insure that the security mechanisms are in place and operating properly (this will include attempts to access the WLAN by devices and applications not authorized to use the WLAN).
5. Test the WLAN on a regular basis noting potential problems and vulnerabilities.
6. Maintain liaisons with all vendors of products used in or on the WLAN to make certain that everything is updated to latest possible revision levels.
7. Develop the ability to determine when new security mechanisms are developed and when their use will enhance the security of the WLAN.

Statements of Applicability

All of the different ISO17799 Controls were closely examined to determine importance to obtaining HIPAA compliance, and to the set up and securing of EcFac's WLAN capabilities, the nature of the applications and data running on (and accessible via) the WLAN, the value to the expansion plans of the Company, and the affect of working toward regulatory compliance (in this case the major issue was HIPAA). In an ideal world, a large percentage of them could be shown to be applicable, even to the WLAN subsystem. The practicality of the matter, however, dictates that focus must be placed on a small percentage of key controls due to time and resource constraints. The

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

following two sections cover the Statement of Applicability for a control that was selected and for one that was not selected.

ISO 17799 Section 12.1.4 … Data Protection and Privacy of Personal Information

- Description – This control concerns the collection, processing and dissemination of personal information. The control proposes the appointment of a data protection officer that would provide guidance to the organization on what data needs to be protected and what procedures need to be followed to accomplish the required protection. It also references the responsibility of the "data owners" in this regard.
- Reason for Selection – Since the Company is subject to regulatory action requiring the privacy of personal data (in this case HIPAA and ePHI) this control is applicable.
- Implementation – This control will be fully implemented
- Justification for Non-Applicability – N/A
- Tools and Methods – This control will be implemented through the —
    - Creation of one or more policies covering the handling of protected data in storage, in processing and during transmission
    - HIPAA Privacy and Security Assessments will be conducted to determine adherence to this control
    - Initially, the CSO will take on this responsibility while it is determined whether a separate Chief Privacy Officer position will be created
- Comments – This will be a major area of discussion during the Company's HIPAA assessment

ISO 17799 Section 12.1.2 … Intellectual Property Rights

- Description – This control states "Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trade marks."
- Reason for Selection – N/A
- Implementation – This control will not be implemented as a part of the HIPAA compliance and WLAN control system implementation efforts.
- Justification for Non-Applicability – The Company has taken the position that it will develop a general policy concerning copy rights and other intellectual property. Any hardware and software containing vendor specific intellectual property will be covered under that policy.
- Tools and Methods – Part of corporate-wide intellectual property policy.
- Comments – Part of corporate-wide intellectual property policy.

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

ISMS Audit Plan (PDCA … Check)

Of those controls reviewed above, six of them were deemed critical to the success of meeting the Company's Business Objectives. The follow sections delineate each of the selected controls and the auditing of these controls.

ISO 17799 Section 4.1.1 … Management Information Security Forum

- Audit Questions –
  - Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organization.
- Reason of Importance – Security is so important to any organization, that it is absolutely necessary to make it extremely visible within the Company. One of the best ways to do this is to make management's commitment highly visible through their support of the Security Management Team (the "Security Forum"). Further, this forum will have representation from all major operational units within the Company.
- Expectations for Compliance – Departmental compliance in the Security Forum is mandatory … there are no exceptions. The "work products" generated by the Forum and its subcommittees (some of which will involve other personnel in addition to the Team members) will be provided to the employees, contractors and other partners of the Company on an "as needed" basis. This is necessary due to the fact that certain documents (e.g. processes and procedures) if allowed into the wrong hands could compromise security.
- Audit Process Steps/Results/Compliance –

Audit Steps	Findings	Compliance
1. Does a Security Forum exist?	The Security Management Team was created by senior staff.	Yes
2. Does the Forum have the correct representation?	Senior staff required the permanent representation from all major departments within the Company.	Yes
3. Does the Forum have a charter that has been accepted by senior management?	The Forum has made this a top priority item on their task list.	No In-process
4. Does the charter provide for[7] — Reviewing and approving information security policy and overall responsibilities? Monitoring significant changes in the exposure of information assets to major threats?	The charter is in development and will include all of these points.	No In-process

[7] Comments in steps 4, 5 and 7 are restated from section 4.1.1 of ISO17799

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

Audit Steps	Findings	Compliance
5. Does the charter provide for — Reviewing and monitoring security incidents? Approving major initiatives to enhance information security?		
6. Is there one "manager" should be responsible for all security related activities?"	Senior management has stated that the CSO will be responsible for managing the Security Team	Yes
7. Does the Forum promote security within the organization through appropriate commitment and adequate resources?	Senior management created the Team and has mandated representation to the Team from all major departments.	Yes

ISO 17799 Section 12.1.1 … Identification of Applicable Legislation

- Audit Questions –
  - Whether all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.
  - Whether specific controls and individual responsibilities to meet these requirements were defined and documented.
- Reason of Importance – This control was considered the most important of all of the ones selected due to the very nature of the information that would be processed over the WLAN and the potential for using the WLAN by an intruder to gain access to the Company's IT infrastructure and the data contained therein. Regulatory requirements such as HIPAA mandate the privacy of certain personal information and provides for severe penalties should an individual's information be illegally obtained or exposed to the public. Penalties exist for both willful and accidental violations and include fines and imprisonment.
- Expectations for Compliance – Compliance with this control is mandatory. The viability of EcFac is dependent upon determining the regulatory requirements that it will be expected to adhere to and the proper execution of its business under the shadow of these regulations. Financial damages (both from governmental agencies and private interests), criminal penalties and loss of reputation are all possible if there is a failure to comply.
- Audit Process Steps/Results/Compliance –

Audit Steps	Findings	Compliance
1. Has the Company identified all major regulatory exposures?	Several regulations have been identified at the federal level including HIPAA and GLBA.	No In-process
2. Has the company obtained copies of applicable regulations?	Copies have been obtained of HIPAA and GLBA rules. Others will be acquired as identified.	No In-process
3. Has the compliance deadlines been determined?	Only in the case of HIPAA and GLBA.	No In-process

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

Audit Steps	Findings	Compliance
4. Have compliance checklists been developed?	No compliance assessment programs have been developed.	No
5. Have compliance assessment programs been developed?	No checklists or project plans have been developed.	No
6. Has the need for outside assessment assistance been determined?	The Forum has determined that in all cases, assessment support from outside organizations will be required due to lack of internal expertise.	Yes
7. Have outside assessment organizations been identified and placed under contract?	The Forum is working with organizations such as FALA to this end.	No

ISO 17799 Section 12.1.4 … Data Protection and Privacy of Personal Information

- Audit Questions –
  - Whether there is a management structure and control in place to protect data and privacy of personal information.
- Reason of Importance – As noted in the previous audit point, regulatory requirements such as HIPAA mandate the privacy of certain personal information and provides for severe penalties should an individual's information be illegally obtained or exposed to the public. Penalties exist for both willful and accidental violations.
- Expectations for Compliance – Again, as noted above, compliance with this control is mandatory. Financial damages (both from governmental agencies and private interests), criminal penalties and loss of reputation are all possible for failure to comply.
- Audit Process Steps/Results/Compliance –

Audit Steps	Findings	Compliance
1. Have all of the regulations affecting the confidentiality of personal information been identified?	This effort is still underway by the Security Forum.	No In-process
2. Have all elements comprising private or protected personal information been identified?	Even though there are gaps in identifying applicable regulations and the need for data privacy therein, the IT department has started a program to insure that all software applications and databases holding any form of personal information have been identified.	No In-process

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

Audit Steps	Findings	Compliance
3. Have the storage locations, processing activities and data transmission regarding the above identified information been identified?	Again, even though there are gaps in identifying applicable regulations and the need for data privacy therein, the IT department has started a program to insure that all hardware devices and software applications have the appropriate security features identified and enabled.	No In-process
4. Have provisions been made to secure the data in the areas noted in item 3 above?	This will occur after the steps in items 1 through 3 have been completed.	No In-process

ISO17799 Section 9.4.3 … User Authentication for External Connections

- Audit Questions –
  - Whether there exist any authentication mechanism for challenging external connections.
- Reason of Importance – Because WLANs use RF technology, their signals often propagate beyond the immediate confines of the facility where they are located. This makes them open to interception by authorized and unauthorized individuals and systems. The WLAN in this case will be carrying ePHI and therefore needs to be secured against unauthorized access.
- Expectations for Compliance – It is expected that the WLAN within EcFac will be maintained in a secure state. It will be available to individuals who have the need for authorized access and "closed" to others. WLAN technology includes a number of security mechanisms to safeguard reduce unauthorized access and to minimize interception of the information carried over the WLAN. This audit will insure that the WLAN including devices and applications utilizing it are properly set up from a security perspective. In addition, since the world of WLAN security is constantly evolving, it is necessary that individuals within the Company for maintaining the WLAN and its security stay abreast of all security upgrades and enhancements. Material from references [15], [8], and [10] were used in the development of this control.
- Audit Process Steps/Results/Compliance –

Audit Steps	Findings	Compliance
1. Is there a policy and accompanying procedures set up for maintaining the security of the WLAN?	The initial policy has been written, but additional work on it is required. In addition, all of the procedures for set up and maintaining the security of the WLAN have to be generated.	No In Process

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

Audit Steps	Findings	Compliance
2. When the WLAN hardware devices are installed and set up, are the security features properly configured?	The WLAN has not been installed and set up yet, so this will be done at that time. As a minimum, the following security details will be established — • The SSID will be set to an ambiguous value • WEP will be set up for 128 bits • MAC filtering will be enabled and the addresses of all devices to be connected to the WLAN will be entered into the MAC Address Tables • A VPN will be set up for the WLAN and all devices connected to the WLAN must have the appropriate VPN client software installed	No This will occur at time of set up
3. Is there a formal WLAN audit and assessment capability in place and exercised on a regular basis?	A formal system will be created and scheduled for regular testing. The system will set up on a specific laptop PC that will be maintained is a secure location. Only individuals with WLAN audit rights will have access to this PC. As a minimum, the following tools will be used on this system — • NetStumbler • Airopeek WLAN audits will occur weekly.	No To be scheduled
4. Is there a procedure in place for maintaining and checking WLAN transaction logs?	When the system is installed and set up, a transaction log will be set up to monitor all transactions occurring over the WLAN. The logs will be scanned on an hourly basis automatically and any attempt at access by an intruder will trigger an alert to the network administrator.	No To be scheduled
5. Is there a mechanism in place in addition to the above logging system to detect intruders coming into the network via the WLAN?	The Company has an Intrusion Detection System in place monitoring the Company's network. The system has to be upgraded to monitor activity coming in from the WLAN gateway.	Yes Updates required

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

Audit Steps	Findings	Compliance
6. Is there a system in place to insure that insures that equipment and software updates from vendors whose product make up or utilize the WLAN are received and acted on in a timely fashion?	Such a system will be set up for the WLAN. It will be managed by the appropriate personnel in the IT department.	No To be scheduled
7. In there an on-going process in place to insure that the individuals responsible for maintaining the WLAN are kept aware of the latest security technology for WLANs?	The need for this activity is well known by the Security Management Team. They Team has budgeted for the periodic training of the analysts who maintain the WLAN.	No In Process

ISO 17799 Section 3.1.1 … Information Security Policy Document

- Audit Questions –
  - Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.
  - Whether it states the management commitment and set out the organizational approach to managing information security.
- Reason of Importance – Proper methods must be documented and put into place to insure that the company is secure in its efforts of handling personal and corporate data and information. The policies that will be developed will insure that the execution of security related tasks and program are consistent. This applies to the determination of regulatory requirements, protection of data and the use of the WLAN within the healthcare environment.
- Expectations for Compliance – A significant amount of work needs to be done to develop the required policies in the areas of regulatory compliance, protection of private (and corporate) information, and in the securing of the WLAN and the information flowing over that portion of the network. In addition, it is imperative that all employees know those policies for which they have the responsibility for as far as enforcement is concerned.
- Audit Process Steps/Results/Compliance –

Audit Steps	Findings	Compliance
1. Does an inventory exist of what security related policies are in place within the Company?	The IT security engineer has accomplished this.	Yes
2. Does a standard template exist that will be used for all security policies?	A standard template from SANS.org has been selected.	Yes
3. Has a role based distribution list been developed for the policies?	This list is in development.	No In-process

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

Audit Steps	Findings	Compliance
4. Has a distribution medium been set up for the security policies?	The Team has determined that the policies will be made available over the Company's intranet using a role-based access control list.	No In-process
5. Has a verification system been developed that will identify each individuals receipt and retention level of the policies?	The team is looking for at several products to assist in this area. One product that appears to meet all of their needs in the VigilEnt Policy Center from NetIQ.	No In-process

ISO 17799 Section 6.2.1 … Information Security Education and Training

- Audit Questions –
  - Whether all employees of the organization and third party users (where relevant) receive appropriate Information Security training and regular updates in organizational policies and procedures.
- Reason of Importance – The only way to make certain that security policies work is to insure that all personnel who have the responsibility for their execution have the policies, understand what their roles are in executing the policies, and what sanctions are in place for failure to comply.
- Expectations for Compliance – Individuals within the organization including employee (full-time and part-time), consultants, management personnel and contractor organizations (e.g. the janitorial service, the document destruction service, etc.) will be required to acknowledge that they have received the policies, understand them and understand their responsibilities in their enforcement.
- Audit Process Steps/Results/Compliance –

Audit Steps	Findings	Compliance
1. Does a mechanism exist to insure that staff members, consultants and others having policy responsibilities have received their policies and understand their role in the enforcement of the policies?	As noted in the audit oversight for the previous control, the Security Forum is looking for at several products to assist in this area. One product that appears to meet all of their needs in the VigilEnt Policy Center from NetIQ. In addition, all employees are given access to the policy section of the Company intranet at their time of employment and are expected to sign an acknowledgement that they have read and understand the responsibilities.	No In-process

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

Audit Steps	Findings	Compliance
2. Will this mechanism insure that the awareness and training mandates of regulations such as HIPAA be met?	If the findings noted in step one above are adhered to, then the mandates will be met and will be verifiable.	No In-process
3. Has this mechanism been put in place?	Not at this time.	No In-process
4. Is there a mechanism in place to insure that responsible parties are made aware of changes to existing policies and new policies are available for their use?	The mechanism selected to accomplish step one above will also satisfy this requirement.	No In-process
5. Do the above mechanisms provide feedback to management that responsible parties fully understand their roles?	The mechanism selected to accomplish step one above will also satisfy this requirement.	No In-process

© SANS Institute 2004, Author retains full rights.

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

ISMS Maintenance and Improvement (PDCA … Act)

On-going Improvement Plans for EcFac's ISMS

The Information Security Management System is currently in development within EcFac … the corporate objectives have been laid out, the risks to the objectives have been identified, and the Security Management Team (the Security Forum) is being put in place. A detailed scheduled has been laid out for the overall ISMS program and is being executed. The projected completion date for the availability of the ISMS is consistent with the overall timeline for Phase I of the Company's expansion program.

Once the initial project is complete, there will still be a significant amount of work left. Security management is a continuous effort … it does not have a finite start nor stop time. It must be in the back of everyone's mind, all the time. Policies will evolve and be enhanced on a continuous basis. New equipment will be added, new personnel will be hired, and new regulations will come into being as time goes on that can affect what is already in place.

In effect, the Company has begun its journey through a continuous security loop using the Plan-Do-Check-Act cycle implicit in international standard ISO17799 for Information Security Management Systems (ISMS). Each pass through the cycle (on a macro-level and using multiple micro-level activities) will refine the ISMS and insure its on-going value to the Company.

The following major activities will be conducted on an on-going basis —

- Keeping aware of new regulatory efforts and changes to existing ones
- The refinement of the Company's Incident Management System (IMS)
- The refinement of the Company's Change Management System (CMS)
- The Development of a Business Continuity Planning process (BCP)
- Creation of a dedicated Security Awareness Program (SAP)

Regulatory Awareness Program

Due to the potential problems brought about by not being aware of regulatory actions that affect the company, the ISMS will evolve to include policies creating methods and assigning responsibilities for identifying and staying current with regulatory affairs that have a direct impact on the Company. It is envisioned that the position of Senior Compliance Officer will eventually be created and that policies in the ISMS related to regulatory affairs will be assigned to that individual.

The initial effort within the Company is being directed at HIPAA. The groundwork laid out working toward HIPAA compliance will be useful in understanding and responding to changes in regulations and the introduction of new regulations.

Incident Management

At this time, the Company does not have an extensive Incident Management System (IMS) in general, and even less when it comes to managing the WLAN. The security engineer from the IT department is currently responsible for responding to IT security

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

incidents, but this is presently done in an ad hoc fashion and she has limited knowledge and experience with wireless networks. The formalization of the Incident Management function will include processes for dealing with incidents involving the WLAN.

Work will be performed to develop controls consistent with sections 6.3, "Responding to Security Incidents and Malfunctions" and 8.1.3 "Incident Management Procedures" of the ISO17799 standard.

Change Management

Change management will evolve in several areas including —

- The ISMS will be placed under the Company's Change Management System (CMS). All changes including additions, corrections, revisions and deletions to the ISMS will be monitored under the CMS. All departments that have changes in their responsibilities when the ISMS changes, will be included in the Change Review process. By placing the ISMS under Change Management, changes to the system will be tracked and approved. The Change Management System will also synchronize with the Company's training and awareness system to insure that ISMS changes are broadcast to everyone with responsibilities under the ISMS.
- Changes to information processing facilities, networks, systems and applications will be controlled in conformance to the ISO17799 specifications for Operation Change Control (section 8.1.2). Such changes are some of the greatest causes of failures in information technology, especially in the area of security.
- Changes in the above areas will be subject to the requirements of ISO17799 section 10.5.1, "Change Control Procedures."

The Security Management Team will be responsible for the implementation of policies and controls in accordance with ISO17799 concerning change management.

Development of a Business Continuity Planning Process (BCP)

ISO17799 calls for the development and maintenance of a Business Continuity Management process (ISO17799 section 11). In addition, HIPAA requires that a Business Contingency Plan, HIPAA standard 164.308(a)(7), be developed as a part of the compliance process. As the Company goes through its expansion plans, increases its geographic presence, brings on more employees, etc., a BCP will become of paramount importance.

The Security Management Team has identified the development of a BCP as a key task to be accomplished as a part of the Company's Phase 2 effort. The planning for the task will occur in the fourth quarter of CY2004.

Development of a Dedicated Security Awareness Program

Very little exists formally within the Company concerning the actions of keeping up with the overall world of IT security. Once the CSO has been brought on board, that individual will be tasked with the creation of a formal security awareness, training and certification program for all current and future employees that have major security responsibilities. Include in this program will be the determination of specific individuals

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

within the company that will need outside training and certification to be successful in their positions.

The CSO and the Security Management Team will work with the Human Resources department to this end. The initial effort will be on the selection, installation and operation of an integrated employee policy awareness system. This system will be used to —

- Warehouse the Policies of the ISMS
- Provide for the creation of new policies, their review and approval
- Distribute of all policies to individuals responsible for their execution on an "as-needed" basis (making sure that dissemination is handled on a required-to-know basis)
- Keep records on which policies were distributed to each employee, the acknowledgement of receipt of these policies, and the retention testing of all individuals of the policies for which they have received and are responsible for
- Generate reports to Human Resources, to departmental management and to senior management on the effectiveness of the awareness program
- Distribute periodic policy updates and reminders to all employees

© SANS Institute 2004, Author retains full rights.

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

References

[1] Department of Health and Human Services, Office of the Secretary. "Health Insurance Reform: Security Standards." United States Federal Register, Volume 68 Number 34; February 20, 2003; Washington, DC. 8334 – 8381.

[2] Novelli, William D. "How Aging Boomers Will Impact American Business." AARP. URL: http://www.aarp.org/leadership/Articles/a2003-01-03-agingboomer.html (21 February 2002)

[3] Breidenbach, Susan. "Howdy, Partner: PBX, WLAN and Handset Makers Step Together to Choreograph Voice-Over Wireless Solutions." NetworkWorld. May 3, 2004 (2004): 41 - 43.

[4] Vocera Inc. "Vocera Communications: HIPAA Data Security and Privacy Standards for Voice Communications Over a Wireless LAN."
URL: http://www.vocera.com/pdf/HIPAA_White_Paper_R4.pdf (17 May 2004).

[5] Breidenbach, Susan. "VoWi-Fi: Early Adopters Deploy Voice Over Wireless to Gain Mobility and Cost Savings." NetworkWorld. May 3, 2004 (2004): 44.

[6] Culler, David E. and Mulder, Hans. "Smart Sensors to Network the World." Scientific American. June 2004: 84 - 91.

[7] Want, Roy. "RFID: A Key to Automating Everything." Scientific American. January 2004: 56 – 65.

[8] Peikari, Cyrus and Fogie, Seth. Wireless: Maximum Security. Indianapolis, IN: Sams Publishing, 2003. 30 - 33.

[9] HCi of Australia. "From Problem Faced to Problem Solved."
URL: http://www.hci.com.au/hcisite2/toolkit/pdcacycl.htm (Date unknown)

[10] Hoesing, Michael and Raval, Vasant. "Using Wireless Audit Techniques." Information Systems Control Journal. Volume 3, 2004: 39 – 42.

[11] CSO Online. "Who is the Chief Security Officer?" CXO Media Inc., IDG (International Data Group).
URL: http://www.csoonline.com/research/security_exec/cso_role.html (2004)

[12] Author Unknown. "Job Description … Manager, Facility Operations" University of New Mexico
URL: http://jobdescriptions.unm.edu/jdeweb.cfm?action=viewSpecific&HRJOB_ID=2766 (December 4, 2002)

[13] Corcoran, Brian. "Wireless Communications Policy." SANS Institute Security Policy Project. July 10, 2003

[14] SANS G17799 Course Material. "Time Based Analysis". Risk Management, Security Compliance and Audit Controls. Pp. 50 - 62. (2003)

[15] Barken, Lee. How Secure is Your Wireless Network. Upper Saddle River, NJ: Prentice Hall PTR, 2004. 4 - 8.

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

[16] International Standards Organization. "International Standard ISO/IEC17799: Information Technology – Code of Practice for Information Security Management." December 1, 2000.

[17] Borkin, Sheldon. "The HIPAA Final Security Standards and ISO/IEC 17799." SANS Institute, Practical Assignment for GIAC GSEC Certification. July 15, 2003.

© SANS Institute 2004, Author retains full rights.

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

Appendix "A" … Proposed Policies

The following policies have been developed by the Security Team and are in the approval process —

1. Wireless Communications
2. Regulatory Compliance

© SANS Institute 2004, Author retains full rights.

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

Title: Wireless Communications Policy

1.0 Purpose
This policy prohibits access to <Company Name> networks via unsecured wireless communication mechanisms. Only wireless systems and applications that meet the criteria of this policy or have been granted an exclusive waiver by InfoSec are approved for connectivity to <Company Name>'s networks.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of <Company Name>'s internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to <Company Name>'s networks do not fall under the purview of this policy. It further covers all software applications that communicate over the wireless LAN.

3.0 Policy
3.1 Register Access Points and Cards
All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by InfoSec. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with InfoSec

3.2 Approved Technology
All wireless LAN access must use corporate-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication
All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.4 Setting the SSID
The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

3.5 Testing the Wireless LAN
The integrity of the WLAN will be tested on a regular basis using the most current version of the WLAN Vulnerability Assessment Procedure <Document Number>

3.6 Applications
All software applications that run on the Company's wireless devices and that transfer data over the wireless LAN must be certified by InfoSec

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

5.0 Responsible Organization
The Network Engineering Team within the Information Technology Department will be responsible for the management and execution of this policy.

6.0 Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

7.0 Revision History
July 10, 2003, Section 3.4 Added
July 6, 2003, expanded to support CDI Initiative, Stephen Northcutt
May 20, 2004, added Sections 3.6 "Applications" and 5.0 "Responsible Organization"; changed subsequent section numbers

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

Title: Regulatory Compliance Policy

1.0 Purpose
This policy establishes the framework for identifying and maintaining compliance with local, state and federal regulations that directly affect the Company.

2.0 Scope
This policy applies to all local, state and federal regulations that affect the operation of the Company.

3.0 Policy
3.1 Identified Regulations
The following regulations have been identified as being applicable to the operations of EcFac —
- Health Insurance Portability and Accountability Act (HIPAA) regarding healthcare information
- Gramm-Leach-Bliley Act (GLBA) regarding financial information
- Sarbanes-Oxley (SOX) regarding corporate financial data

3.2 Employee Responsibility Regarding Confidentiality of Personal Information
Under no circumstances are employees allowed to release any form of personal information to individuals or organizations outside of the Company unless a Resident Release of Information is on file within EcFac and specifically releases the requested information.

3.3 System Requirements Regarding Confidentiality of Personal Information
All servers, databases and applications containing or processing data that could be classified as "private" must have the appropriate protective controls in place and activated.

3.4 Identification of New Regulations or Changes to Existing Regulations
A constant watch will be conducted to determine if new regulations or changes in current regulations will affect the company.

4.0 Responsible Organization
The Security Management Team will designate a "regulatory compliance" committee to perform this function until such time that a Senior Compliance Officer has been hired or appointed. At that time, the SCO will take over the responsibilities for this policy. The regulatory compliance committee or the Senior Compliance Officer will be responsible for identifying new regulations or changes to previously known regulations that would have an effect of the Company.

5.0 Enforcement
Individuals within the Company who violate this policy will be subject to immediate personal sanctions up to and including "discharge with cause" from the Company. Any employee finding a security issue with any of the Company's servers, applications, databases or networks detecting a vulnerability that could result in the loss of personal data must report it immediately to their supervisor, who in turn must report it to the Incident Response Team.

6.0 Definitions

Terms	Definitions
HIPAA	Health Insurance Accountability and Portability Act
ePHI	Electronic Protected Health Information

7.0 Revision History
Policy created May 24, 2004

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

Appendix "B" …HIPAA Security Standards; Final Rule

Standards [1]	***Sections***	***Implementation Specifications (R)=Required (A)=Addressable***
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

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

Standards [1]	***Sections***	***Implementation Specifications (R)=Required (A)=Addressable***
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

© SANS Institute 2004, Author retains full rights.

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

Appendix "C" Key Security Employee Job Descriptions

Chief Security Officer

(Derived from "Sample CSO Job Description" created by CSO Online [11]*)*

This is the top security executive in the company. He or she will report directly to the CEO. The CSO will oversee and coordinate security efforts across the company, including information technology, human resources, communications, legal, facilities management and other groups, to identify security initiatives and standards. The candidate will work closely with the chief information security officer and must have working knowledge of information technology.

Responsibilities:

- Act as the chairperson for the Security Management Team
- Oversee a network of employees and vendors who have the responsibilities to safeguard the company's assets, intellectual property and computer systems, as well as the physical safety of employees and visitors.
- Identify protection goals and objectives consistent with corporate strategic plan.
- Manage the development and implementation of global security policy, standards, guidelines and procedures to ensure ongoing maintenance of security under the auspices of ISO17799.
- Maintain relationships with local, state and federal law enforcement and other related government agencies.
- Oversee the investigation of security breaches and assist with disciplinary and legal matters associated with such breaches as necessary.
- Work with outside consultants as appropriate for independent security audits.
- Understand and manage compliance efforts for all required regulatory affairs such as HIPAA and GLBA.
- Create and manage a formal security awareness, training and certification program within EcFac.

Qualifications:

- Must be an intelligent, articulate and persuasive leader who can serve as an effective member of the senior management team and who is able to communicate security-related concepts to a broad range of technical and non-technical staff.
- Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.
- Ability to communicate effectively, both orally and in writing.
- Skill in organizing resources and establishing priorities.
- Ability to provide technical leadership and direction to technical and support staff.
- Desirable to have some background in law, law enforcement or intelligence.
- Must have a solid understanding of information technology and information security (including firewalls, VPNs, penetration testing and other security devices.
- A security certification such as CSEC or CISSP is required.

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

Facilities Security Manager

(Derived from "Manager, Facility Operations Job Description" created by University of New Mexico [12]*)*

Under limited supervision from the Chief Operating Officer, manages all aspects of the integrated facility security operations and services of the Company which will eventually occupying multiple geographically separated sites. The Manager will oversee the supervision of security guards and resources at the various corporate sites. The Manager will plan, oversee, and coordinates the implementation of security related capital improvement projects, and directly participates in the Security Management Team.

Responsibilities:

- Provides technical leadership for integrated physical plant security activities and programs of the company, to include security component maintenance and construction, guard services, and support of the Security Management Team.
- Develops and establishes policies and objectives consistent with those of the organization to ensure secure operation of all EcFac facilities.
- Oversees the supervision of security personnel, which includes work allocation, training, and problem resolution; evaluates performance and makes recommendations for personnel actions; motivates employees to achieve peak productivity and performance.
- Oversees the activities of external and/or internal contract security personnel; monitors and inspects work to ensure adherence to contract specifications and industry standards.
- Develops or assists with the development and implementation of policies and procedures consistent with those of the organization to ensure efficient and safe operation of the residents, the company, and the employees.
- Develops and implements systems to maintain records on employees, security equipment inventories, and compliance activities.
- Establishes and maintains appropriate security services procedures and standards; interfaces with residents and employees and resolves problems and conflicts as necessary.
- Remains available to the component on a 24-hour, 7-day on-call basis as principal respondent to physical plant emergencies and off-standard situations, as required.
- Oversees the development and implementation of physical security, safety, and disaster recovery programs, procedures, and operations for the company.
- Consults and interacts with community fire, police and medical response organizations.

Qualifications:

- Skill in examining and re-engineering security operations and procedures, formulating policy, and developing and implementing new strategies and procedures.
- Ability to communicate effectively, both orally and in writing.
- Skill in organizing resources and establishing priorities.
- Ability to provide technical leadership and direction to technical and support staff in a range of physical plant trades.
- Ability to supervise and train staff, including organizing, prioritizing, and scheduling work assignments.

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

- Knowledge of all federal, state, and local codes and ordinances pertinent to facilities security planning, design, construction, and maintenance.
- Ability to develop and implement facility safety, security, and disaster recovery programs and procedures.
- A security certification such as CPP or PSP is required.

© SANS Institute 2004, Author retains full rights.

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

Last Updated: May 25th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced