CASE MODEL

THE SEARCH FOR A CHIEF SECURITY OFFICER

The Mighty-Soft Hospital is a futuristic 1,500 bed fortress-like facility operating with a state-of-the-art dual wired-wireless infrastructure complete with computerized physician order entry system, radio frequency inventory device (RFID) control tags, and integrated electronic medical records (EMRs) that are the envy of its competitors and vendors, and offer a formidable strategic competitive advantage in the marketplace.

Now, imagine the potential liability, PR disaster and chagrin when its *enfant terrible* CEO is told of a massive security breach similar to the ChoicePoint and Lexis-Nexis fiascos. The ID theft involves release of critically protected healthcare financial, employment, clinical, and contact information for all of its patients, employees, physicians, business associates, and affiliated medical personnel.

Suddenly, senior management is charged with the task of establishing the new position of Chief Security Officer (CSO) for Mighty-Soft, and navigating a crisis management dilemma never previously faced by the formerly HIPAA-compliant electronic giant.

The CSO is to be a senior level management position responsible for championing institutional security. Awareness of electronic and HIPAA policy and procedure developments, while working to ensure compliance with internal and external standards related to information security, is vital. The CSO is to report directly to the CEO and the CIO.

The Search Committee developed the following list of CSO duties and responsibilities:

- Chair the hospital's ***Information Security and Privacy Committee*** in its policy development efforts to maintain the security and integrity of information assets in compliance with state and federal laws, and accreditation standards.
- Provide project management and operational responsibility for the administration, coordination, and implementation of ***information security policies*** and procedures across the enterprise-wide hospital system.
- Perform periodic ***information security risk assessments*** including disaster recovery and contingency planning, and coordinate internal audits to ensure that appropriate access to information assets is maintained.
- Work with the financial division to coordinate a ***business recovery plan***.

- Serve as a ***central repository*** for information security-related issues and performance indicators. Research security or database software for implementing the central repository, and note that a server based system could be useful for a Wide Area Network (WAN), so this information can be shared with the enterprise-wide hospital system. Develop, implement, and administer a coordinated process for response to such issues.
- Function when necessary as an approval authority for platform and/or application security and coordinate efforts to ***educate*** the hospital community in good information security practices.
- Maintain a broad understanding of ***federal and state laws*** relating to information security and privacy, security policies, industry best practices, exposures, and their application to the healthcare information technology environment.
- Make recommendations for short- and long-range security planning in response to future systems, new technology, and new organizational challenges.
- Act as an advocate for security and privacy on internal and external committees as necessary.
- Develop, maintain, and administer the security budget required to fulfill organizational information security expectations.
- Demonstrate effectiveness with consensus building, policy development, and verbal and written communication skills.
- Possess the clear ability to explain information technology concepts to audiences outside the field.
- Become the public face for the Mighty-Soft Hospital's legacy security system.

Minimum Qualifications:

- Bachelor's degree in Computer Science or related field or equivalent experience.
- Three or more years of experience in the healthcare industry.
- Five or more years of experience in information security.
- Eight or more years of experience in information technology.
- In-depth understanding of network and system security technology and practices across all major computing areas (mainframe, client/server, PC/LAN, telephony) with a special emphasis on Internet related technology.

Preferred Qualifications:

- Experience with electronic medical devices.
- Specific experiences in the healthcare industry.
- Familiarity with legislation and standards for PHI and patient privacy.
- Demonstrated successful project management expertise.
- Professional certification, *e.g.*, CISSP, CISA, PMP.
- Experience with student record/higher education laws.

KEY ISSUES:

What is your IT hardware infrastructure and how are security-related devices deployed?

What security requirements are imposed by federal and state authorities on your institution?

What would you consider the most important criteria for choosing a CSO?

What relationship will the CSO have with the CIO, CMIO and CEO?

What level of security education/training do you consider necessary for your hospital community?

What are the key security issues your CSO will have to address?

What are the key privacy issues?

What are the key risk management issues?

What are the pros and cons of EHRs for your institution?

What do you see as the EHR priorities for your CSO?

What are the security issues of EHRs for your institution?

<