The Importance of Healthcare IT Security

Charles O’Brien

September 16, 2010

Abstract

Implementing technology in a secure manner is an important issue in the health care industry. To remain effective and efficient, businesses require electronic solutions to be put into operation. Furthermore, the United States Government currently offers incentives to early adopters of certified technology programs and will penalize health care providers who do not embrace specific technologies in the near future. Healthcare organizations have already started to move toward storing and transmitting sensitive patient data electronically. Information Technology (IT) solutions must be implemented and maintained with solid security design and proper risk management. The goal of this research paper is to educate healthcare providers about the importance of effective security planning and operations. This paper will discuss the important challenges that IT professionals face to ensure the security of systems and the privacy of patients. In a poignant observation of security, the reformed computer criminal Kevin Mitnick insists that a company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets, hired building guards from the best security firm, followed every best-security practice recommended by experts, slavishly installed every recommended security product, and been thoroughly vigilant about proper system configuration, but the company would still be totally vulnerable to attackers (Mitnick, 2002). When a well-respected security expert makes a statement of this caliber, healthcare professionals should consider the serious predicament the healthcare industry confronts.

Table of Contents

Table of Figures

Introduction

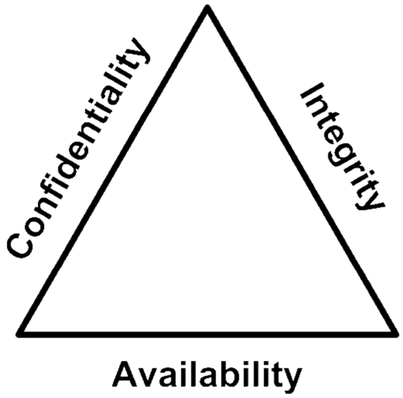
The confidentiality of information exchanged in a doctor-patient relationship is of vital importance to the proper functioning of the healthcare industry. Technology is introducing new challenges to maintaining the privacy, integrity, and availability of health data. Until recently, the healthcare industry has not been a large target for attackers. This industry has flown below the hacker radar primarily because sensitive data has been contained in a physical paper chart. Technology allows for health information to be stored and transmitted in bulk, which creates a potentially high-value target for malicious individuals and organizations.

The threats involved in protecting a paper chart versus protecting an electronic chart are very different. A paper chart may be copied or stolen; an entire electronic database containing many patient charts may be copied or deleted. Compounding the situation, attacks from the internet may be carried out anonymously, thus creating a large reward-to-risk ratio. It is essential that medical providers recognize the security implications that technology brings to healthcare.

The Function of Security

The goal of effective security design is to ensure the Confidentiality, Integrity and Availability of systems and data. This basic model (known as the CIA triad) is widely agreed to represent the core principles of information security. Here is a further breakdown of definitions:

Figure 1. The CIA triad



- Confidentiality ensures information is disclosed only to authorized users. A security breach may threaten the privacy of patient data and sensitive business information.

- Integrity ensures that data is accurate and complete. Inadequate integrity controls may lead to data tampering and disastrous decision making.
- Availability ensures up-time and usability of systems for authorized users. If critical systems are not readily available, normal business operations may not proceed.

A functional security program is beneficial to both physicians and patients. Since nearly everyone plays the role of patient during their lifetime, physicians should be aware of both perspectives. Privacy benefits for a patient include the ability to avoid forms of exploitation such as fraud, identity theft, blackmail, targeted advertisements, embarrassment, and discrimination. Medical data is one of the most personal and private types of information humanity possesses. Life threatening conditions, drug abuse, psychological issues, and abortion are several examples of sensitive health information that may be exploited by identity thieves, insurance companies, employers, and governments. Many benefits of privacy and security exist for patients, but ethical, legal, and business reasons also exist for physicians.

Ethical commitments.

Historically, physicians swear an oath which addresses privacy when starting to practice medicine. This oath from circa 400 B.C. translated from Greek asserts:

> Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private (The Hippocratic Oath).

Legal mandates.

Within the United States, the Federal Government mandates health information privacy. The recent adoption of electronic medical records has highlighted the need for new regulations to protect individually identifiable health data. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has been regularly amended to address new concerns of electronic data having an increased potential for access and abuse. The official description of HIPAA states:

> The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. (Health Information Privacy)

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), which is part of the American Recovery and Reinvestment Act of 2009, extends the security and privacy requirements of HIPAA with regard to electronic communication of health information. The new rules require security breach notification, heightened enforcement, increased penalties, and the introduction of audits (Acevedo, 2009).

Business requirements.

A security violation may lead to the disclosure of sensitive business information including patient data, financial data, and intellectual property. Theft of trade secrets and other proprietary information may result in loss of income, reputation, and competitive edge, all of which could be disastrous for a business. Industrial espionage, foreign governments, and malevolent hackers target the data of organizations with aspirations of profit. Senior management establishes the organization’s computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. Ultimately, the head of the organization is responsible for ensuring that adequate resources are applied to the security program and that it is successful (Roles and responsibilities, 2007).

The ultimate goal of achieving secure healthcare systems is to protect patients and physicians from the many threats that the health industry will face due to modern widespread acceptance of health information technology. Sensitive healthcare systems may contain vulnerabilities and therefore be exploited by attackers if security is not suitably implemented. Fortunately, risks may be identified, assessed, and managed appropriately with careful cost-benefit analysis. When the significant impact of security is understood and risks are properly managed, healthcare and information technology are able to provide quality care to patients and maintain the confidentiality, integrity, and availability of patient data.

Specific Challenges and Solutions

Healthcare providers may not understand the complexity or the significance of implementing secure electronic systems. Many challenges must be addressed to protect patient data from loss and theft. Once patient data is stolen and published, this disclosure cannot be reversed. Often, security is not prioritized or completely avoided for multiple reasons:

- Implementing security initially takes time and effort to institute.
- Vendors purposely disable security mechanisms and prohibit security practices because secure systems are more difficult to troubleshoot.
- Healthcare providers and vendors lack incentives.
- Personnel lack education and understanding of consequences.

Security threats to healthcare organizations must be addressed to ensure proper functioning of the healthcare industry. Because security threats and new technologies constantly evolve, this paper will offer solutions to the most significant security challenges.

Challenge 1 - Lack of Security Education

Effective implementation of security mechanisms is largely dependent upon the education of individuals in an organization. Security is as much of a management issue as it is a technical issue. Since security typically restricts a user's abilities, the benefits of applied security should be understood for maximum adoption. A successful healthcare security plan includes participation from physicians, management, and all supporting staff.

Support from senior management is vital to the success of a security plan, so security should be addressed in business terms. Management is not interested in technical jargon, but instead is interested in the likelihood of security incidents, what their impact may be, and what mechanisms may be put in place to handle these concerns. If the importance of security as a whole is understood, the organization will realize the importance of the next two challenges: effective security planning and a sufficient IT security budget.

Challenge 2 - Lack of Effective Security Planning

The purpose of security planning is to prepare for, prevent, and if necessary, recover from a security breach. Ultimately, the best way to protect an organization is to prevent security incidents from occurring in the first place. This goal is possible with effective security planning.

To ensure that risks are known and managed, the company should develop a formal security policy to identify security requirements and protection mechanisms. A security policy is vital since it will formally assert the intent of management to protect its information assets. This document will aid in the ability to make decisions and achieve sensible outcomes.

A security policy must be adhered to in order to be effective, but unfortunately policies are sometimes disregarded. A survey sponsored by Symantec, which questioned healthcare IT security professionals, found that three quarters of organizations that conduct formal risk assessments found patient data at risk due to inadequate security controls, policies, and processes (Symantec, 2009). Organizations should analyze security periodically to confirm that their desired security baseline standards are being maintained.

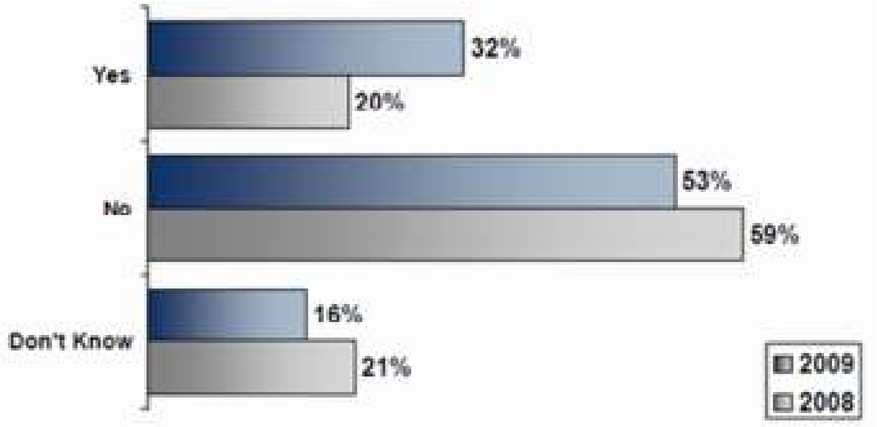


Figure 2. Instances of medical identity theft. Reprinted from "HIMSS Security Survey," by Symantec, 2009, 2nd Annual HIMSS Security Survey. Copyright 2009 by Symantec. Reprinted with permission.

Effective security is implemented with a proactive and multi-layered approach. Effective security planning should address common issues and follow best practices:

- Implement defense in depth strategies
- Apply the principle of least privilege
- Hire knowledgeable security professionals or outside consultants
- Design network architecture while prioritizing security

- Software developers should design software securely
- Require authentication to access systems
- Log and review security relevant data
- Maintain up-to-date software patches for all enterprise software
- Maintain up-to-date anti-virus
- Utilize encryption for sensitive data in transit and at rest
- Conduct security audits (Businesses that fail to conduct security audits do not know the quality of their security profile)

Challenge 3 - Insufficient IT Security Budgets

All too often, security is perceived as a nuisance. Businesses understand the need to protect their assets, but protection mechanisms are often postponed because risks are not understood, counter-measures cost money, and systems rarely generate income by being more secure. Generally companies invest in security *after* having an unfortunate security breach. As more companies are experiencing data breaches, they are responding in a reactive way, rather than proactively reviewing the company's security to find vulnerabilities (Jewellap, 2007).

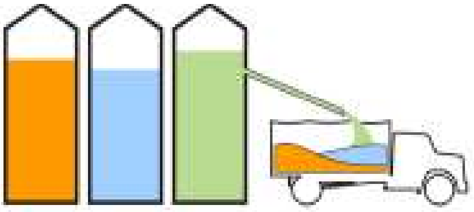
Security is oftentimes included as an additional responsibility of the IT department. Businesses may have in-house IT staff, but these professionals are typically busy with day-to-day operations and not educated in security. Security is a distinctive field which requires specialized knowledge and keeping up with current trends. The assumption that IT departments will implement systems securely is incorrect. Security is a separate responsibility that should have its own resources.

Challenge 4 – Attackers Target Enterprise Databases

In *Database Servers: Candy for Hackers,* Ericka Chickowski (2009) offers insight explaining why attackers target large databases: “good hackers today are business people, assessing each target for the simplest and most profitable attack scenarios. These days, there are probably no plumper targets than enterprise databases” (para. 1). With the increasing rate of targeted attacks, the goal of hackers to make money, and the wide-scale adoption of electronic health records, the rate of attacks targeting medical databases will continue to rise.

The storage of patient data is shifting from being widely distributed in paper charts to being housed electronically in data silos. Electronic databases are particularly important to properly secure since a large amount of sensitive data will be stored in one place. Once a database is stolen, it may be analyzed by competitors, sold to insurance companies, published on peer-to-peer file sharing networks, or countless alternatives. Large stolen databases historically wind up being published and freely downloadable on the Internet.

Figure 3. Harvesting data from a large silo is more convenient for an attacker than if the data were distributed

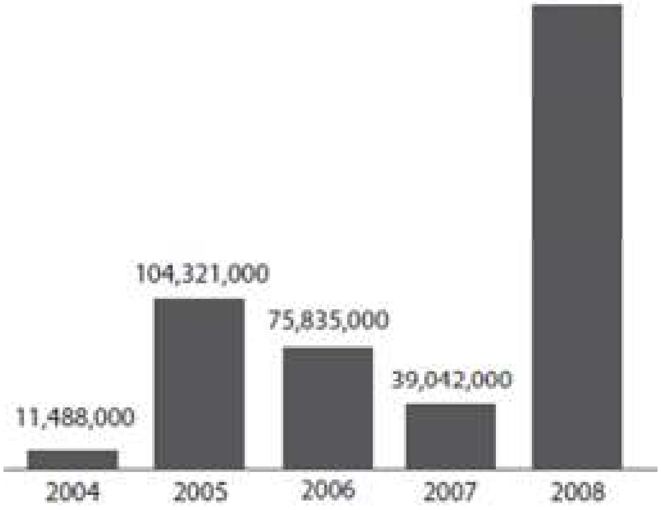


- 6,000 Social Security numbers of Harvard applicants were compromised and publically shared in a compressed 125 Megabyte file via BitTorrent, a peer-to-peer network (Vamosi, 2008).
- 60,000 user names and passwords were stolen from a scam Web site designed to look like MySpace. Later that data was made available from a popular security mailing list (Niranjan, 2007).
- 570,000 pager messages intercepted during the September 11 attacks are currently published by WikiLeaks (9/11 tragedy pager intercepts).

Because the Internet lacks physical boundaries, healthcare security is an international issue once technology is involved. The National Health Service in England acknowledges that confidential patient information has been lost in numerous cases. Files, computers and memory sticks containing details of thousands of patients have been lost, according to details released because of the Freedom of Information Act (Russell, 2008). Recognizing the potential risk to patient confidentiality, "in Germany, the national association of doctors in private practice (NAV Virchow Bund) has adopted a stance advocating the complete abandonment of all concepts of central data storage in the German national health IT project" (Grätzel, 2008, para. 2).

Hackers, businesses, and governments will always covet large and sensitive databases. Deborah Peel, the founder of Patient Privacy Rights Foundation observes, "If privacy is not fully protected, we won't be building anything except the most valuable mother lode of information for data mining on Earth" (Foreman, 2006). Verizon's Business RISK team reports that 285 million database records were stolen in 2009 (Baker, et al.). To put this number in perspective, this was the population of the United States in July of 2001 (Population Estimates).

Figure 4. Number of database records compromised per year. Reprinted from "2009 Data Breach Investigations report," by Baker, et al., 2009, Copyright Verizon Business.



Challenge 5 - Many Attack Vectors Exist

The main challenge of securing systems is maintaining the fine balance between security and productivity/utility. New healthcare technologies allow for improvements of accuracy, speed, and communication in patient care. Technology increases value by helping businesses remain up-to-date and competitive. The addition of new features and technologies increases the attack surface of an organization and therefore also increases the undertaken risk. A commentary from Derek Gabbard (2010), the CEO of a security company, clarifies the importance of minimizing attack surface:

> As an analogy, when a martial artist squares off against an opponent, he positions himself in a way that best reduces his attack surface. He must consider his entire body as part of the attack surface. He shifts his stance, maintains balance, and positions his arms and hands up in order to protect his vital points. While everyone has their fair share of vulnerabilities, those that are successful in protecting themselves, do a better job minimizing their exposure. (para. 2)

As technology is introduced into healthcare environments, security should be analyzed and risks properly managed. Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories: avoidance, mitigation, transfer, and acceptance (Dorfman, 2007). Security professionals identify weaknesses, predict how a malicious person would abuse technologies, and subsequently minimize these risks.

Generally, people recognize the threat of malicious hackers, but many security breaches are the result of accepted *features* that increase risk as a side-effect:

- Wireless
- Email
- Removable devices
- Portable devices (phones, PDAs, etc.)
- Environment
- Trusted employees
- Third party service providers

Third party vendors introduce vulnerabilities.

All too commonly, third party vendors introduce vulnerabilities and increase the threat surface area of medical organizations. The Verizon Business RISK team reports that business partners were the source of 32% of confirmed security breaches in 2009 (Baker, et al.). Third-party vendors, motivated by income, are interested in installing new systems and increasing their market share. Given that secure systems are more difficult to maintain, numerous medical vendors purposely disable security mechanisms and have the audacity to *prevent* security implementations because of requirements due to contracts or warranties. Consumers of third-party services and products should be aware of this issue and manage their increased risk accordingly. Common varieties of compulsory restrictions include:

- Administrative permissions for users
- Prohibition of additional policies
- Disabled firewalls
- No operating system updates
- No anti-virus

Challenge 6 – Advanced Persistent Threats

Advanced Persistent Threats (APT), a common buzz-term in the security community, is the realization that modern attackers are automated, return-on-investment focused, and multi-layered. APTs are launched by skilled attackers whose goal is to cause severe economic disruption to the business and to gather intelligence in a targeted manner (Cisco 2010 midyear security report, 2010). These attacks are designed to remain under the radar of system administrators and security protection mechanisms. After gaining a foothold inside of a company's network, an attacker will attempt to remain entrenched in order to steal company secrets or other data. This year, a wave of attacks targeting more than 20 large U.S. companies including Google, Adobe, and other companies aspired to steal valuable intellectual property (Drummond, 2010). As the adoption of technology in the medical industry increases, so will the rate of this class of targeted attacks.

Conclusion

Technology is constantly introducing new challenges to information assurance and security. Organizations need to recognize the important role of security in healthcare environments to ensure their systems properly function. Healthcare organizations will continue implementing technical solutions at an enormous rate in the upcoming years. Emerging technologies and software will customarily result in increased attack vectors as security researches uncover new vulnerabilities. Since targeted attacks against healthcare organizations and large databases in general are on the rise, protection mechanisms should be adopted early. Unfortunately, as in the case of trade secret theft, once medical data is stolen (and possibly published) this theft cannot be undone. As more medical data is electronically accumulated and exchanged, physicians will have an increased responsibility for maintaining secure systems.

Bibliography

9/11 tragedy pager intercepts. (n.d.). Retrieved September 7, 2010, from WikiLeaks: http://911.wikileaks.org/files/index.html

Acevedo, L. (2009, February 24). *Stimulus package dramatically alters HIPAA privacy and security.* Retrieved August 31, 2010, from Wisconsin Technology Network News: http://wistechnology.com/articles/5558/

Baker, W. H., Hutton, A., Hylender, C. D., Novak, C., Porter, C., Sartin, B., et al. (n.d.). *2009 data breach investigations report.* Retrieved September 7, 2010, from Verizon Business RISK team: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Chickowski, E. (2009, June 20). *Database servers: Candy for hackers* . Retrieved September 6, 2010, from Information Week: http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=218100141

Cisco 2010 midyear security report. (2010). Retrieved September 8, 2010, from Cisco: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_mid2010.pdf

Dorfman, M. S. (2007). *Introduction to Risk Management and Insurance (9 ed.).* Englewood Cliffs, N.J: Prentice Hall.

Drummond, D. (2010, January 12). *A new approach to China*. Retrieved September 8, 2010, from The Official Google Blog: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Foreman, J. (2006, June 26). *At risk of exposure.* Retrieved August 31, 2010, from Los Angeles Times: http://articles.latimes.com/2006/jun/26/health/he-privacy26

Gabbard, D. (2010, August 5). *Attack Surface Expanded by Extended Enterpris.* Retrieved September 8, 2010, from Security Week: http://www.securityweek.com/attack-surface-expanded-extended-enterprise

Grätzel, P. (2008, January 16). *German doctors say no to centrally stored patient records.* Retrieved September 7, 2010, from eHealth Insider: http://www.e-health-insider.com/news/3384/german_doctors_say_no_to_centrally_stored_patient_records

Health Information Privacy. (n.d.). Retrieved July 23, 2010, from U.S. Department of Health & Human Services: http://www.hhs.gov/ocr/privacy/

Jewellap, M. (2007, December 30). *Record number of data breaches in 2007.* Retrieved September 7, 2010, from MSNBC: http://www.msnbc.msn.com/id/22420774/

Mitnick, K. D. (2002). *The Art of Deception.* Indianapolis: Wiley Publishing Inc.

Niranjan. (2007, January 19). *60000 MySpace username passwords stolen.* Retrieved September 7, 2010, from Security Tools News & Tips: http://securitytnt.com/60000-myspace-username-passwords-stolen/

Population Estimates. (n.d.). Retrieved September 7, 2010, from U.S. Census Bureau: http://www.census.gov/popest/national/national.html

Roles and responsibilities. (2007, July 6). Retrieved September 6, 2010, from NIST Special Publication 800-12: An Introduction to Computer Security: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter3.html

Russell, B. (2008, November 26). *Catalogue of NHS data losses makes shocking reading.* Retrieved September 7, 2010, from The Independent: http://www.independent.co.uk/life-style/health-and-families/health-news/catalogue-of-nhs-data-losses-makes-shocking-reading-1035166.html

Symantec. (2009, November 3). *2009 HIMSS Security Survey.* Retrieved September 1, 2010, from Symantec: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-himss_security_survey_11-2009.en-us.pdf

The Hippocratic Oath. (n.d.). Retrieved August 31, 2010, from United States National Library of Medicine: http://www.nlm.nih.gov/hmd/greek/greek_oath.html

Vamosi, R. (2008, March 13). *Harvard student database hacked, posted on BitTorrent.* Retrieved September 7, 2010, from CNet: http://news.cnet.com/8301-10789_3-9893174-57.html

Wagner, M. (2009, November 10). *Healthcare providers face security challenges.* Retrieved August 17, 2010, from Information Week: http://www.informationweek.com/news/healthcare/security-privacy/showArticle.jhtml?articleID=221600842