Chapter 6
Is Your Automated Healthcare Information Secure?

Mhamed Zineddine
AlHosn University, UAE

ABSTRACT

Information security issues are a serious matter that organizations from all industries have to deal with. The healthcare industry is no exception. Personally identifiable healthcare information automated by the healthcare industry can be stolen, intercepted, altered, and misused. Acceptable safeguards, therefore, have to be in place in order to ensure the privacy and protection of this information. Without governmental intervention however, it seems unlikely that the healthcare industry will voluntarily implement such safeguards. The Health Insurance Portability and Accountability Act (HIPAA) security rule has emerged and been mandated by Congress from the need of such intervention. The quantitative investigation in this chapter is aimed at determining if covered entities in Washington State are HIPAA security rule ready after two years from the compliance deadline, and if the factors identified through the literature review are a hindrance to HIPAA security rule compliance. This research study revealed that HIPAA Security Rule full compliance is far from achieved; many factors have emerged as impediments to the compliance process, and the way to compliance is complex and costly. Tracking the compliance progress within healthcare institutions in Washington State over the last five years revealed that the reaction to the HIPAA Security Rule was strong around the mandated date; the response after the mandated date, however, has been weak. Covered entities should brace themselves to the new level of enforcement due to the recent American Recovery Reinvestment Act (ARRA).

INTRODUCTION

Information Technology (IT) has become a core part of every business. As Bruce (1998) explains, IT has become a salient enabler of business strategies in areas of mass customization, competitive differentiation, quality improvements, and process automation and improvement. IT affects the entire spectrum of retail, manufacturing, and service companies including healthcare institutions. Nowadays, organizations operate in a dynamic, fast-changing environment due to a number of

DOI: 10.4018/978-1-61350-123-8.ch006

factors, such as technical innovations, new and creative ideas, strategic alliances, acquisitions and mergers, and a culture of continuous change (Ekstedt et al., 2005). The information assets of organizations have been stored mostly in a digital format. As Qu (2001) points out, these assets include the intellectual property, products, as well as classified and private information about business partners and customers. Modern business practices require that these assets have to be available, reliable, and accessible by customers, employees, and partners on site and at a distance. Because the digital world in which these assets are stored (cyber-space) is as vulnerable to attack as it is accessible. It is dangerous to store valuable data in this environment. Securing these information assets is crucial and a leading priority of responsible management, especially IT managers in healthcare establishment. "Security" to these leaders is closely connected to, if not synonymous with, "disaster recovery" of information assets (Johnson, 2002).

The aim of planning, designing, and implementing Information Technology (IT) security best practices is not only to ensure the confidentiality and the integrity of the data produced and used, but also to sustain the availability of the Information Systems (IS) (Davies, 1986; Forcht, 1994; Pfleeger, 1997).

The IT security dilemma becomes more relevant when private healthcare information is concerned. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") enacted by Congress was designed to improve portability and continuity of health insurance coverage in the group and individual markets. The HIPAA security rule is a step towards standards that would ensure the security and integrity of patients' information stored or transmitted electronically or what is called electronic private healthcare information (ePHI).

The security requirements and rules mandated by HIPAA focus both on external and internal security threats. Contrary to popular conception, however, the internal threats are at least equal external problems as security concerns and are far more likely to occur according to many security experts. The problem is that it is doubtful that healthcare institutions will be able to meet the requirements of the HIPAA security rule to prepare for these threats (Walt, 2004; Bravo, 2005).

BACKGROUND OF THE STUDY

As Information Technology has become a part of the core business in today's organizations and the fabric of our daily lives, the security of private and personal information has become an increasing concern. This concern has evolved as the rate of computer-related crimes has risen especially in the areas of hacking, theft, fraud, sabotage, and cyber terrorism. Changes in cultural, social, economic, and business boundaries make Information Systems (IS) easy to reach. Private and personal information can be remotely targeted. The value of this information makes it attractive to hackers, thieves, and rivals.

Information security, however, has evolved through time alongside the bad guys. Organizations' policies and rules to protect sensitive data have been evolving through careful trial and error over the last 20 years.

Research of computer crimes and security management often suggests poor implementation of security measures and little awareness about security issues. Security and protective measures are implemented in a piecemeal manner, often in response to surfacing security problems or violations. Most employees within organizations and computer users at home are not aware of vulnerable and possible exposure areas that may threaten an organization's or personal information nor do they