MPW-98789_section_1_written_paper

by Glenn Reyn

Submission date: 11-Apr-2019 10:32PM (UTC-0700)
Submission ID: 1110946386
File name: MPW-98789_section_1_written_paper.docx (24.64K)
Word count: 1406
Character count: 8125

CIS 438: Case Study 1: HIPAA, CIA, and Safeguards

Kwaku Adomako

School or Institution Name (University at Place or Town, State)

CIS 438: Case Study 1: HIPAA, CIA, and Safeguards

Information technologies play the role of utilities in our lives. Exponential penetration of information and communication technologies have changed the way people do business. Healthcare systems are no exception to this change. Modern healthcare facilities are powered by rigorous information technology infrastructure to provide efficient service to their clients and patients. An important aspect of the use of information technology in healthcare facilities is the electronic records of patient information (Sessions & Kobus III, n.d.). Most of the time such records contain personally identifiable information of patients and are known as personal health information (PHI) records. Almost all of the departments associated with healthcare facilities use electronic records to maintain and deliver patient information such as diagnostic history and other clinical records along with personal information of the patient.

Storage of personal information of patients in electronic health record systems has made them a potential target of cyber-criminals. They are always developing new and sophisticated attacks to compromise records of personal information. To prevent the breach of personal information and to protect the security and privacy of such records, there is an act known as health insurance portability and privacy (HIPAA) act. HIPAA act outlines various security and privacy safeguards for all of the healthcare facilities providers to secure the information stored in their systems (McMenamin, 2017). It requires the security and privacy guards in place for data security including technical and administrative measures as well. Where each healthcare facility provider claims to be the best to protect patient information, the headlines are filled with news of successful security breaches of such organizations. One such example is the breach experienced by the Blue Cross Blue Shield of Tennessee (BCBST).

BCBST is a healthcare insurance provider company and as per the nature of business records and maintains personal health information of their clients. In 2009, the insurance provider suffers a data breach due to negligence and non-compliance with HIPAA act. The breach of BCBST involves a massive amount of 57 hard disk drives containing personal health information of almost one million people. The breach was settled with the United States Department of Health and Human Services (HHS) for $1.5 million. The penalty was imposed due to noncompliance with the HIPAA act by the BCBST. HIPAA act requires the healthcare service providers to store user data in encrypted storage devices to protect the confidentiality, integrity, availability, and non-repudiation of data. As per the HIPAA act, confidentiality means that personal health records of patients must not be visible to unauthorized parties (Hsieh, 2014). The organization is responsible to make essential deployments to protect such information from breaches. Integrity requires that the information must not be tampered with and availability requires that the information must be available to authorize parties when required.

BCBST failed to implement these requirements of data security required by the HIPAA act. The hard drives containing personal health records of patients, recordings of support providers, and voice recordings of collaboration with executives were stolen from a leased facility. The breach signifies that there were no physical access restrictions were applied by the BCBST to protect the unauthorized access to critical information technology infrastructure. Therefore, the attackers were able to physically breach the system and compromised physical media containing critical information assets of the insurance provider (Janardhanan, 2013). Investigations further revealed that the company has not implemented the encryption of data as required by the HIPAA act to protect the confidentiality and integrity of data. Encryption is the process of securing the data with the encryption key and only the parties having the key can

retrieve original information from the storage system. BCBST revealed that the data on hard drives was encoded but not encrypted using an encryption algorithm and that was a potential violation of HIPAA act that resulted in a massive financial penalty.

When data in storage systems is encrypted using any of the encryption algorithms available in the market the attackers cannot decode original data even if they are aware of the underlying encryption algorithm. An encrypted system is as secure as the associated key of encryption. BCBST was not using any encryption system and key management system as well. As the settlement of the breach and payment of the penalty, the BCBST agreed to review its privacy and security policies (Huq, 2015). They agreed to perform a system-wide audit and overhaul of the existing security infrastructure of their system. BCBST partnered with Kroll Inc. a leading data security service provider to restore the identity theft conditions. They started rolling notifications to the members and provided customer support through live call facilities. In case, a member has reported the misuse of stolen identity supported by medical bills was offered a restoration service with the help of Kroll.

BCBST agreed to strengthen existing security measures of the leased space that was breached in the attack. It also agreed to conduct training of employees and gradual compliance check by the HHS for increased security of data. They deployed an encryption mechanism that allowed them to ensure the confidentiality and integrity of stored data in their systems. However, if all of such measures introduced earlier, the breach would not happen in first place. The logical measures accepted for implementation by the BCBST are good to protect the data logically but administrative reforms are required as well. BCBST agreement on implementation of logical security can raise the security bar significantly but they completely neglected the possibility of insiders attack on their infrastructure (Rose & Rose, 2014). An insider attack is one in which an

employee of the company can breach the system for various reasons. Insider attacks can only be prevented through administrative reforms and regular training of the employees.

Physical security is inevitable in critical data protection strategies as all of the logical measures can be rendered useless if a system can be breached physically. Physical access restriction must be applied for the employees as well. There must be appropriate data segregation between the organizations as well such that the finance department would not be able to access data of the sales department. BCBST installed network level firewalls to protect its network from hackers but they neglected the possibility of attack from within the network (Cavanaugh, 2018). Firewalls only consider attacks from outside of the network. Any compromised host inside the network will continue to perform its malicious actions regardless of the firewall protection. Intrusion detection and prevention system must be implemented by the BCBST to protect the systems against such attacks.

In successful data breaches, the organizations not only suffer from financial losses but more severe reputation loss as well. Reputation loss is the most difficult to restore when the breach involves personal and private information of millions of people. As per HIPAA act, every organization dealing with personal health information of patients must use encryption and enterprise key management systems (Cortez, 2018). They must conduct employee training regularly to educate them about new features of installed security systems to protect critical user information. As the data stored in systems is the most critical asset of any healthcare organizations it is their obligation to ensure compliance with HIPAA act. Along with logical reforms physical protections must be in places such as administrative restriction and comprehensive security and privacy policies.

References

Cavanaugh, D. (2018). Protecting Your Practice: A Guide to Medical Malpractice Coverage. *The Journal of Medical Practice Management: MPM*, *33*(5), 314–317.

Cortez, N. (2018). The Evolving Law and Ethics of Digital Health. In *Digital Health* (pp. 249–269). Springer.

Hsieh, R. (2014). Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment. *Loy. U. Chi. LJ*, *46*, 175.

Huq, N. (2015). Follow the data: Analyzing breaches by industry. *TrendLabs Research Paper*.

Janardhanan, R. (2013). Uncle Sam Knows What's in your Medicine Cabinet: The Security and Privacy Protection of Health Records Under the HITECH Act. *J. Marshall J. Info. Tech. & Privacy L.*, *30*, 667.

McMenamin, J. (2017). The Law of Telemental Health. In *Career Paths in Telemental Health* (pp. 15–39). Springer.

Rose, R. V., & Rose, L. H. (2014). Appreciating healthcare data privacy laws in Canada, the United Kingdom, and the United States. *EDPACS*, *49*(5), 18–24.

Sessions, L., & Kobus III, T. J. (n.d.). *The Anatomy of a Healthcare Data Breach*.

MPW-98789_section_1_written_paper

ORIGINALITY REPORT

9%	7%	3%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Lynn University Student Paper	3%
2	www.coursefortune.com Internet Source	3%
3	LexisNexis Publication	2%
4	en.wikipedia.org Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		