IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 10, Issue 4 (May. - Jun. 2013), PP 83-87
www.iosrjournals.org

Road Map to HIPAA Security Rules Compliance: Risk Analysis at Orbit Clinics

Muhanned Z Alaqili
College of Business, Lewis University, USA

Abstract : *The organization, which will be used in this risk assessment report, is a healthcare provider and concealed name "Orbit Clinic" is to protect confidentiality and anonymity of the real clinic's name. This assessment will look at the clinic IT systems only from HIPAA Security Rules point of view. This clinic has chosen because there are various threats and vulnerabilities, which are faced by these kinds of organizations especially regarding the electronic Personal Health Information (e-PHI). They also have sensitive financial data that need to be secured due to the possible threats and vulnerabilities facing them. The analysis approaches that have used are interviews, survey, automated tools like Zenmap and Nessus. In addition, Methodologies such as quantitative, qualitative and Practical Threat Analysis (PTA) were used to conduct the risk analysis. As a result, to this risk assessment, quite a number of vulnerabilities were observed. Furthermore, the project provided countermeasure to all observed vulnerabilities as well as the most cost effective plan to mitigate the risks.*
Keywords: *Risk Analysis, Practical Threat Analysis, Risk Management, Nessus*

I. Introduction

Organized risk management could be said to have at least as early as the first time a king or a Lord decided to fortify walls, store extra provisions in case of famine or make security alliance by having the buyers provide safely. Babylon was also the birthplace of banking, where lenders managed risks starting with careful selection of debtors. During that period through the Middle Ages, risk management was an unguided mitigation of risks. Choosing what risks to prepare for was always matter of gut feel. The development of probability theory and statistics in the 17th century allowed the risk to be quantified in meaningful way. However, at that time it was adopted only in selected industries for selected applications. By 1940s, more sophisticated risk assessments were applied to and even developed by nuclear power and oil exploration. This was facilitated by the development of computers and the ability to generate random scenarios with quantitative models. But until the end of 20th century, risk management was not even on the radar of most organizations (Hubbard, 2009). Health Insurance Portability and Accountability Act of 1996 (HIPAA) simply protects the privacy of individually identifiable health information. There are new rules were created by HIPAA for sharing and using health information. Privacy, Security and Administrative Simplification are the new rules and have major impact on all covered entities the U.S.A. The HIPAA Security requirements were issued on February 20, 2003. Small health entities were given until April 21, 2006 to achieved compliance. Otherwise, non-compliance fees will be applied. Fees can be $100 to $250.000 and 10 years jail time (Kairb, 2004).

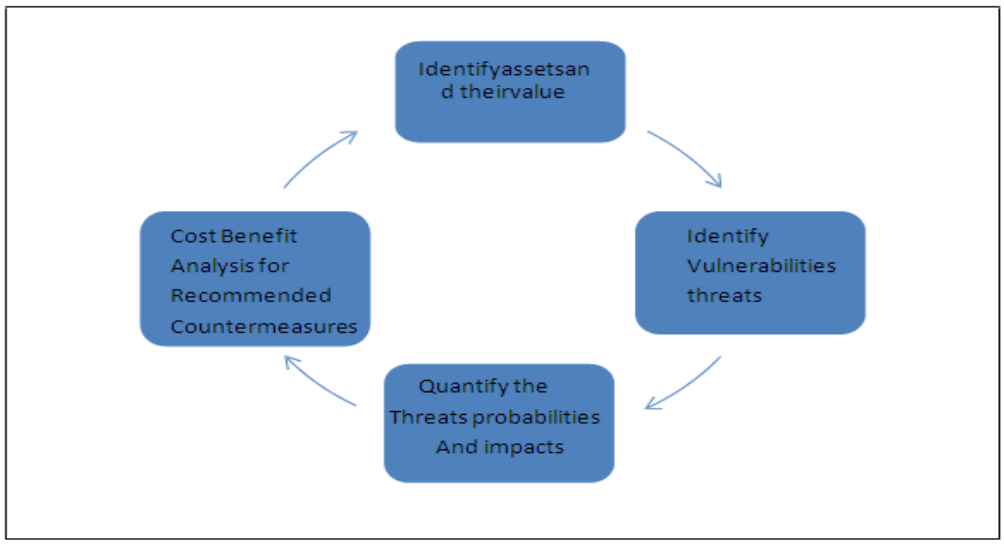
(E-PHI) includes any medium used for data at rest (storage) or in transit involving PHI. [4] For instance:

Media containing data at rest (storage)
Personal computers with their internal hard drivesused at work, home, or traveling
1.1 External portable hard drives, including iPods and similar devices,
Magnetic tape
1.2 Removable storage devices, such as USB memory sticks, CDs, DVDs, and floppydisks
1.3 PDAs and smartphones

Data in transit***, via wireless, Ethernet, modem, DSL, or cable network connections***
1.4 Email
1.5 Filetransfer

Risk analysis main goals

Figure 1. Risk analysis main goals



As shown in Fig 1, risk analysis has four main goals (Harris, 2012) which is Identify assets and their value to the organization, Identify vulnerabilities and threats, Quantify the probability and business impact of these potential threats and Provide an economic balance between the impact of the threat and the cost of the countermeasures

1.5 Identify assets and their value to the organization

Understanding the value of an asset is the first step to understand what security mechanisms should be put in place and what funds should go toward protecting it. If a company does not know the value of the information and the other assets it is trying to protect, it does not know how much money and time it should spend on protecting them.

1.6 Identify vulnerabilities and threats

Once the assets have been identified and assigned values, all of the vulnerabilities and associated threats need to be identified for each asset or group of assets.

1.7Quantify the probability and business impact of these potential threats

We need to calculate the probability and the frequency of the identified vulnerabilities being exploited. Additionally, we need to gather information about the likelihood of each threat that takes place.

1.8 Provide an economic balance between the impact of the threat and the cost of the countermeasures

The last step is to identify countermeasures and solutions to reduce the potential damages from the identified threats

II. Methods

The project utilized different approaches and automated tools like Qualitative, Quantitative (Tan, 2002), and Practical threat methodologies (Ygor Goldberg, 2007)to gatherand analyze information as follows:

2.1 Interviews and security survey conducted by using a special tool provided by NIST (National Institute of Standards and Technology) called HSR (HIPAA Security Rules) toolkit (The National Institute of Standards and Technology (NIST), 2009). The sources of information used to support the development of the HSR Toolkit questionnaires include the following:

HIPAA Security Rule

2.1.1 NIST Special Publication 800-66

2.1.2 NIST Special Publication 800-53

2.1.3 NIST Special Publication 800-53A

2.1.4 HealthInformation TechnologyforEconomic andClinical Health (HITECH) Act

2.2 Network discovery Conducted by using Zenmap program (Forlanda, 2012), which is the GUI of Nmap and used to support the manual inventory performed by Orbit Clinics personnel prior the beginning of the project

2.3 Nessus is a web-based application used to scan networks to determine vulnerabilities that can be exploit by hackers (Wendlandt, n.d)

2.4 Practical Threat Analysis (PTA) is computer-based software that helped to assist risk analysis by producing an effective risk mitigation plan (Lieberman, 2012)

III. Calculation

Assigning values to tangible assets was very interested and important phase since all the outcomes of this risk analysis depend on how accurate the assets values are. To find out the overall Dollar amount of an asset certain steps (Tan, 2002) should be followed:

3.1 Interview with the Clinic Manager to find out the cost of the existing assets
3.2 Included costs related to the followings:
3.3 Installation Cost
3.4 Troubleshooting cost
3.5 Added 10% contingency
3.6 Loss of business services to outside customers
3.7 Loss of business services to internal employees

Besides assets pricing, several calculation steps were performed during the analyzing phase some of them were completed manually and the rest performed automatically by PTA (Ygor Goldberg, 2007). *Exposure Factor (EF)* = Percentage of asset loss caused by identified threat; ranges from 0 to 100% addressed as Threat's Damage to Asset in PTA. *Annualized Rate of Occurrence (ARO)* = Estimated frequency a threat will occur within a year and is characterized on an annual basis addressed as Threat's Probability in PTA. *Maximal value of system risk* is the financial value of the risk to the system if no countermeasures are implemented. It is calculated by summing the multiplications ofthe asset's maximal risk by the asset's value for each of the assets in the system. *Minimal Value of system risk* is the financial value of the risk to the system if all countermeasures are implemented. It is calculated by summing the multiplications of the asset's minimal risk by asset's value for each of the assets in the system. *Current value of system risk* is the financial value of the risk to the system taking into account the contribution of countermeasures already implemented.

IV. Results

The project analyzed information systems and recommended controls to mitigate risks to protect electronic personal health information. The results will be used as a baseline for defining and generating controls relative to acceptable use, protection of information and protection of systems. The process included the following: (The Institute for Information Assurance (IIA), 2012)

4.1 A physical investigation of designated location to be familiar with the details of information transmission, storage, and processing
4.2 Interviews with data owner, custodian, and users concerned with administration of hardware, databases, and application programs, to identify processes and loss exposure.
4.3 Assessments of current controls and electronic systems that store, maintain, create, and transmit information.

Table 1. System's Risk Status

System's Risk Status	
Maximal Risk Level	431.3 %
Current Risk Level	304.0 %
Minimal Risk Level	45.6 %

As shown in Table 1, the system's risk status current level is 304% of the total assets value $ 1 094.319

Table 2. Top Five Unmitigated Threats

Threat Rank	**Name**	**Valueat Risk**
1	Attempted Unauthorized System Access byOutsider (Hackers)	$828,084
2	Act of humanerroror failure	$735,740
3	DataIntegrity Loss	$292,768
4	Natural disasters	$268,053
5	Technical software failures or errors	$254,062

As shown in Table 2, the top 5 threats on Orbit Clinic's IT system. The highest threat is hackers with their destructive abilities and the least one on the table is the technical software failure or errors.

Vulnerabilities are unique in any project because they could differ from one location to another and from one application/system to another. Finding vulnerabilities requires intimate knowledge of the location to be able to observe the existing vulnerabilities and thus its countermeasures. Hence, identified countermeasures in this project are based on previous risk analysis conducted by professionals on variousIT systems, security technical reports and background experiences.

Countermeasures cost were estimated based on market prices. For example, providing awareness training to staff can cost nothing if it is conducted online. Some websites offer free training and information regarding security awareness like SANS Securing the human. SANS provides an excellent free security awareness tools such road map poster, videos, and awareness planning kit (SANS, n.d). On the other hand, if the organization would like to provide education for one of its employees the cost of two days course could be $ 2000 (SANS, 2012).

Table 3. The correlation between risks and recommended counter measures

Risk No.	Risk (Threat)	Countermeasures
1	**Software attacks**	Vulnerability/PatchManagement Intrusion Protection Detection System Installanti-DoS appliance Harden Network Devices
2	**Power outage**	Provide emergency power source /Power stabilizer
3	**Communication Loss**	Ad-hoc network
4	**Data IntegrityLoss**	Vulnerability/PatchManagement Control the humidity and temperature of the facility Provide awareness training to staff Provide emergency power source /Power stabilizer Conduct training on the proper and secure use of the system
5	**Act of human error or failure**	Provide awareness training to staff Conduct training on the proper and secure use of the system
6	**Abuse of Access Privileges by Employees**	Enforce quality passwords policy for protecting each of the machines on the network Harden Network Devices Restrict administrator privilege only to administrator
7	**Natural disasters**	Establish off-site Backup Develop, document, implement and test backup procedure

As shown in Table 3, the correlation between risks and recommended countermeasures. Each risk or threat can be mitigated with one or more countermeasures. Furthermore, some of the countermeasures can mitigate several threats. For instance, patch management can mitigate software attacks, data integrity loss, attempted unauthorized system access by hacker technical software or errors and denial of services. Likewise, providing emergency power source or power stabilizer can mitigate power outage.

V. Conclusion

The project followed standardized steps in conducting risk assessments. First, assets that holding (E-PHI) were identified through the physical investigation and inventory list. Next, assets were calculated by using certain steps to determine the right assets value. Then, vulnerabilities were observed and discovered by using HIPAA Security Rule (HSR) and other automated tools. Data owner, custodian and users were interviewed and answered vast number of questions that have different categories: administrative safeguards, physical safeguardsand organizational requirements. After that, the project got the advantage of using automated tools to gather more information about existing vulnerabilities like Zenmap and Nessus. Zenmap was used mainly to discover the network and to support the provided

preliminary inventory list. In addition, Nessus the vulnerability scanner was used to discover IT system's vulnerabilities. Then, all collected information has been analyzed and inserted into (PTA) main classes. Assets, vulnerabilities, threats and countermeasures are the main classes of PTA. Practical Threat Analysis is a calculative modeling methodology and software tool that assists the project in finding out the most cost-effective countermeasures. The project encountered some difficulties like quantifying intangible assets and determining the exact cost ofthe countermeasures.

References

[1] Douglas W. Hubbard, *The Failure of Risk Management*. Hoboken, US: John Wiley & Sons, Inc, 2009.
[2] Sundhansh Kairb, *A Practical Giued to Security Assessments*, 1st ed. Boca Raton, Florida, USA: AUERBACH Publication, 2004.
[3] Shon Harris, *All in-One CISSP Exam Guide*, 5th ed. New York-Chicago-SanFranciso, USA: Timothy Green, 2012.
[4] Ding Tan. (2002, December) Reading Room SANS. [Online]. http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849
[5] Michael Levy Ygor Goldberg, "PTA," US20070016955 A1, 2007.
[6] The National Institute of Standards and Technology (NIST). (2009, May) SCAP Related Publication. [Online]. http://scap.nist.gov/publications/index.html
[7] J. Forlanda. (2012, MAy) Nessus vs Nmap. [Online]. http://www.brighthub.com/computing/smb-security/articles/72408.aspx
[8] Dan Wendlandt. (n.d, n.d) Nessus. [Online]. http://www.cs.cmu.edu/~dwendlan/personal/nessus.html
[9] Danny Lieberman. (2012, July) Excel is not the answer for Risk Assessment. [Online]. http://www.ciozone.com/index.php/Security/Excel-Is-not-the-Answer-for-Risk-%20Assessment.html
[10] The Institute for Information Assurance (IIA), "Will County Community Health Center Risk Analysis," College Of Business, Lewis University, Romeoville, 2012.
[11] SANS. (n.d) Security Awareness Planning. [Online]. http://www.securingthehuman.org/resources/planning
[12] SANS. (2012, December) MGT433: Securing The Human: Building and Deploying an Effective Security Awareness Program. [Online]. http://www.sans.org/event/cyber-defense-initiative-2012/course/securing-human-building-deploying-effective-security-awareness-program
[13] U.S. Department of Health & Human Services. (n.d.) Health Information Privacy. [Online]. http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
[14] Knowledge Base Indiana University. (2012, January) Knowledge Base. [Online]. http://kb.iu.edu/data/ayyz.html
[15] National Institute of Standards and Technology. (2012, March) HIPAA Security Rule Toolkit. [Online]. http://scap.nist.gov/hipaa/
[16] William Miaoulis. (2010, November) A HIPAA Security Overview (Updated). [Online]. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048519.hcsp?dDoc Name=bok1_048519
[17] Randy George. (2012, September) Vulnerability Management. [Online]. http://www.darkreading.com/vulnerability-management/167901026/security/perimeter- security/240007070/a-guide-to-network-vulnerability-management.html
[18] Mick Bauer, "Paranoid penguin: Practical threat analysis and risk management," *ACM Digital Library*, January 2002. [Online]. http://dl.acm.org/citation.cfm?id=512797&bnc=1
[19] Russ McRee. (2008) PTA: Practical Threat Analysis. [Online]. http://holisticinfosec.org/toolsmith/docs/september2008.pdf