Controlling Critical Risks in Healthcare

Sophia Segal* *Director, Business Analyst Solution, Toronto, CANA*

ABSTRACT:

Healthcare is a rapidly growing sector and an active research area which allows doctors to access patients remotely. Today's healthcare automation problem requires different methods to address the issues in security. Both the patient's information and IT infrastructure should be protected. Healthcare automation systems are facing more and more security threads that causes loss or damage of data. As a Risk Analysis and Requirements expert, I understand that IT data requirements is also one of the most valuable assets to a pharmaceutical or healthcare company. Data is key to the whole clinical development process. Without clean data, the value of a project, drug or product may not be fully realized. There are many solutions which reduces vulnerability in health care systems so that it becomes impossible for hackers to compromise the system. If vulnerabilities in the system are not identified, defects become extremely expensive and burdensome to fix and can escalate to critical risk, fast. [16] This paper focuses on critical health care security risks and gives few solutions to overcome and control them.

Keywords: *Healthcare automation systems, security threads, vulnerability in health care systems, risk assessment.*

INTRODUCTION:

Health care is the maintenance or improvement of health via the diagnosis, treatment, and prevention of disease, illness, injury, and other physical and mental impairments in human beings [1]. The objective of healthcare automation is to provide medical services (through remote access) to users irrespective of their location. The clients can access these systems using their home internet. Healthcare is mainly developed to address problems like lack of availability of doctors, lack of advanced medical equipment, and lack of patient history. Almost all countries adopted healthcare automation and got benefit from it [2] [3]. In present systems, it is hard to find a perfect needed medical service, either the patients need to travel a long distance to find the medical service or the medical service may not be efficiently operating and also patients had to wait for long time in order to communicate to the doctor.

The healthcare system consist of connected network of various hospitals, clinics, remote contractors, external parties, suppliers, university. This vast network creates many vulnerability that permits a hacker to enter into the system and access the information without authentication or by providing fake authentication [4] [5].

SOME AREAS WHERE SECURITY CAN BE COMPROMISED:

According to a survey [6], nearly 260 million records are hacked in 2005. Here are some of the scenarios where risks are likely to occur in health care system.

Patients and doctors access the healthcare system through mobile phones or laptops. These electronic devices can be used at any places like inside hospital or at homes, or at public places etc...

Most of the patients have the lack of knowledge to use the health care system. So they require another person to help them in accessing the healthcare system.

There are many open networks proving free internet access. Most of them are unsecure network connections which can easily allow hackers to enter into the system.

Unclean data is also vulnerable to risks. I, as a risk solution expert , implemented critical data validation checks by running technical SQL and SAS queries against the Oracle DBMS to identify deficiencies, including missing data or unclean data and performing a comprehensive risk assessment comprising a thorough root cause analysis of deficiencies and vulnerable risks due to security risks to funnel down where they triggered from and causality which has solved many high risk occurrences happening escalating into crisis recovery situations.

Risk assessment involves identifying the critical systems and business areas most vulnerable to risk, so that resources can be assigned where the risk impact is highest. In this scenario, the highest risk impact has a direct correlation to defects that potentially have serious consequences. For all the risks, assign a score to each one, probability of occurrence and its impact on the user and contingency plans if the risks occur. Compile a risk report, assigning each risk a unique id and a description and review it once a week with the team. Any new risks, derived from open defects, should be raised as they are identified. Other risks can be, and usually are, adjusted in terms of significance as more information comes to the surface about them. [14] But without proper risk analysis, defects surface after implementation, at a time when it costs tenfold to pursue and resolve the same defect. [15]

SECURITY MEASURES:

Experienced in leading IT projects at Loblaw, I carried out tactical risk assessments and mitigation techniques, enhances compliance including identifying threats from critical security risks. This plan involved incorporating a risk assessment and mitigation and applying decision techniques to select relevant risk factors with high predictive values of studies that may be non compliant.

This involved a combination of her technical and risk analysis knowledge, fuzzy processes and leveraging reflective data collection and analysis to identify potential risk factors, which I have detailed in this section.

This section focuses on these security measures that can be taken to prevent hackers into the system. The basic thing to do is to add a custom firewall into the system so that it makes the existing firewall stronger. The two level firewall also makes easier to add custom exceptions. The security implementation are of 3 steps as shown in figure 1. The assessment step is the detail investigation of the presence of vulnerabilities in the system. After the thorough security assessment, the acceptable risk of the healthcare system is created. The acceptable risk is set of vulnerabilities which the system cannot be compromised. It is really difficult for a system to eliminate all the risks, so the acceptable risk is created in such a way that security should focus only on risk that really matters. The control step has a list of actions that brings the risk drown to acceptable risk. The last step is compliance, which involves time to time investigation of the security.

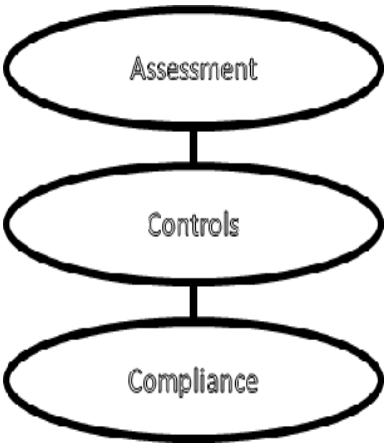

Figure 1: Risk prevention steps

When a new thread is detected, the security team must not only focus on how to prevent it but they should consider more other thinks like where the thread comes, what are the vulnerabilities found, what are the other ways that the thread can compromise the system? The two questions that should be asked after a thread is found is consequence and likelihood. Consequence determine the risk level, whether the thread is acceptable level or not? If the thread is acceptable, then we can skip the evaluation process. The next question is likelihood, how often the thread occurs, if it is too often, then we can add it to the firewall.

Data loss is an important feature that need to be addressed by the healthcare. Data replication [7] is the traditional and one of the best approaches to ensure availability of data during data theft or damage of data [8].

Data in healthcare often travels in many devices like PC, Laptops, Smartphones etc. There are lots of chances for data to reach to hack like usb theft, Laptop theft, email sent to wrong person etc… to avoid these problem the system should implement end to end security system[9]. Implementing end to end encryption has lots of advantages like it stops man in the middle [11] and backdoor attacks [12] [10].

The best way to improve security in health care is to add a new embedded OS. The features of health care should not be accessed in traditional OD like windows, Linux or mac, instead the healthcare system should have its own OS so that it is difficult for hackers to enter into the system. Malware attacks are also impossible in custom OS. One more thing we get from this custom OS is Intrusion protection. Intrusion protection is detecting abnormal activities in the network, stopping them by using pre-configured polices and giving timely report on security attacks. The custom OS should support the configuration of Intrusion protection such that it prevents damages to file system, prevents unauthorized user entry, controls, removable storage devices.

CONCLUSION:

Healthcare is most needed in the future to provide efficient treatment of various diseases, there are various security attacks in healthcare. This paper focuses on various vulnerabilities in healthcare system and provide few solutions to overcome them. Because of the potential for monetary loss or damage to the credibility of an enterprise due to breakdown of its system or infrastructure, businesses have come to realize the importance of investing time and money on risk assessment to not only safeguard the company brand but mitigate monstrous financial losses caused through disaster or incident recovery. [13]

About Author

Sophia Segal is a Senior Management Computer Solutions Analyst, also acting as Computer and Information Research lead advising organizations about

the appropriate strategy in the use of technology solutions to meet their business requirements and mitigating risk in Clinical diagnostics and Healthcare. She has over 20 years consulting experience, specializing in Requirement principals, Risk Management and assessing business-critical risks. She is consulting at Roche International Clinical Diagnostics & Pharmaceuticals.

REFERENCES:

[1] "Health topics: Health systems". www.who.int. WHO World Health Organisation. Retrieved 2013-11-24.

[2] "Health at a Glance 2013 - OECD Indicators" (PDF). OECD. 2013-11-21. pp. 5, 39, 46, 48. (link). Retrieved 2013-11-24.

[3] "OECD.StatExtracts, Health, Health Status, Life expectancy, Total population at birth, 2011" (online statistics). stats.oecd.org/. OECD's iLibrary. 2013. Retrieved 2013-11-24.

[4] Anderson, Nate (February 9, 2011). "How one man tracked down Anonymous—and paid a heavy price". Arstechnica.com. Retrieved March 29, 2011.

[5] Palilery, Jose (December 24, 2014). "What caused Sony hack: What we know now". CNN Money. Retrieved January 4, 2015.

[6] Privacy Rights Clearinghouse. http://www.privacyrights.org

[7] Mansouri, Najme, GholamHoseinDastghaibyfard, and Ehsan Mansouri. "Combination of data replication and scheduling algorithm for improving data availability in Data Grids." Journal of Network and Computer Applications (2013)

[8] Dragan Simic; SreckoRistic; Slobodan Obradovic (April 2007). "Measurement of the Achieved Performance Levels of the WEB Applications With Distributed Relational Database" (PDF). Electronics and Energetics. FactaUniversitatis. p. 31–43. Retrieved 30 January 2014

[9] "Hacker Lexicon: What Is End-to-End Encryption?". WIRED. Retrieved 22 December 2015.

[10] Chris Alexander, Ian Avrum Goldberg (February 2007). "Improved User Authentication in Off-The-Record Messaging" (PDF). Proceedings of the 2007 ACM workshop on Privacy in electronic society. New York: Association for Computing Machinery: 41–47. doi:10.1145/1314333.1314340

[11] Chris Alexander, Ian Avrum Goldberg (February 2007). "Improved User Authentication in Off-The-Record Messaging" (PDF). Proceedings of the 2007 ACM workshop on Privacy in electronic society. New York: Association for Computing Machinery: 41–47. doi:10.1145/1314333.1314340

[12] Goodin, Dan (20 May 2013). "Think your Skype messages get end-to-end encryption? Think again". ArsTechnica

[13] Segal, Sophia (13 March 2017). "Best practices to prevent data breaches.". Risk Management Magazine, http://www.rmmagazine.com/2017/03/13/best-practices-to-prevent-data-breaches/.

[14] Segal, Sophia (03 February 2017). " User Acceptance Testing and the Application Lifecyle". Simple Talk, https://www.simple-talk.com/dotnet/net-development/user-acceptance-testing-application-lifecycle/

[15]] Segal, Sophia(12 March 2017). "A Framework for removing ambiguity from software requirements. IIOAB Journal. ISSN 0976-3104. P 43-46

[16] Segal, Sophia (March 14 2017). "Overcoming poor usability and user Requirements". Test Magazine, p2-4.

.