International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Security Issues with Health Care Information Technology

Ahmed Mohamed Mahmoud[1], Akram M Zeki[2]

[1, 2]Faculty of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia

Abstract: ***Nowadays data become one of most important and expensive things in our life. Whereas life became a huge database, content all information in it. However it is not necessary that data be relate to financial area to be expensive and important. While now and in last period, the healthcare sector has become one of the most vulnerable sectors to hack. Why? It is the question that we should ask to understand well the importance of data that contained in this sector. In addition, How? To know how can we protect this sector from hacking or breach. There are many hospitals and clinic hacked in different countries and by different ways. Whereas Data and Information that stole or hacked, most of it was just personal information not financial information such as credit card. It is because this data become more expensive than financial information. On the other hand, There is a question we must to ask: Why attacking increased just in the last period? Are there any relation between it and the increase of medical devices that are connecting on internet? All of that problems or damages cost healthcare organization each year more and more than we can imagine. Thus, must there solutions with less cost for all of that, maybe they will be not the final solution but at least can decrease the damage that effect healthcare organization each year.***

Keywords: Healthcare industry, security, privacy, cloud computing, data breach, hack

1. Introduction

In the light of attacks on the healthcare industry there must be ways or solutions to repel these attacks by protect data or as it is so-called Data Security. Whereas Data Security is protecting data or database from devastating and from unauthorized actions of unauthorized users. Therefore there are many solutions and technologies created for different kinds of attacking, such as: security system (Data masking, Backups, Disk Encryption), security hardware, and the most important is preparing well the team who is responsible on information division to be ready in any time to resolve any problem.

2. Breaches between Cost and Statistics

There are many cases of hack and breach happened in last period while more than 50% of that attacks occurred in Healthcare entities (Hospitals, Pharmacies, Health Plan, Lab, etc….) in comparison with 14% of attacks occurred Government entities. Healthcare industry in target for many reasons such as: Firstly, Healthcare industry security is not upgradable as fast as other industries. Secondly, personal patient information become more valuable than other information while a healthcare document can sold around 20$ compared with 1$ for credit card numbers. Furthermore, approximately 94% of healthcare organization had at least one data breach in just two years, while the cost of that damage was around 2.4 million dollars. [1] More than that it is not necessary to get the information through hacking, whereas information can found by theft or loss laptops, mobile phones or any storage devices. Especially if that laptops or mobile phones are not protecting with any kind of security such as password or any kind of data encrypting.[1][2]

The pie chart below in Figure 1 shows the percentage of total breaches that occur in different entities.

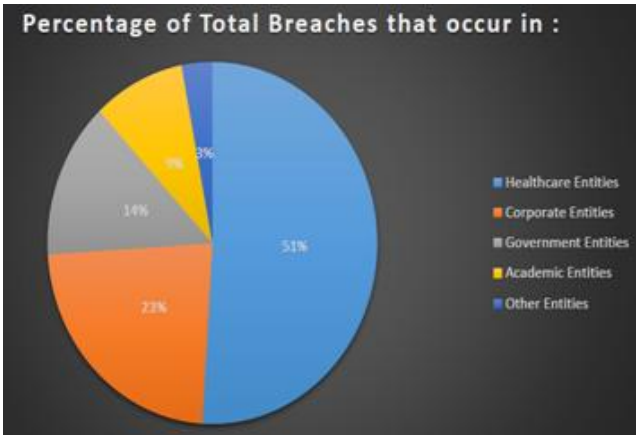
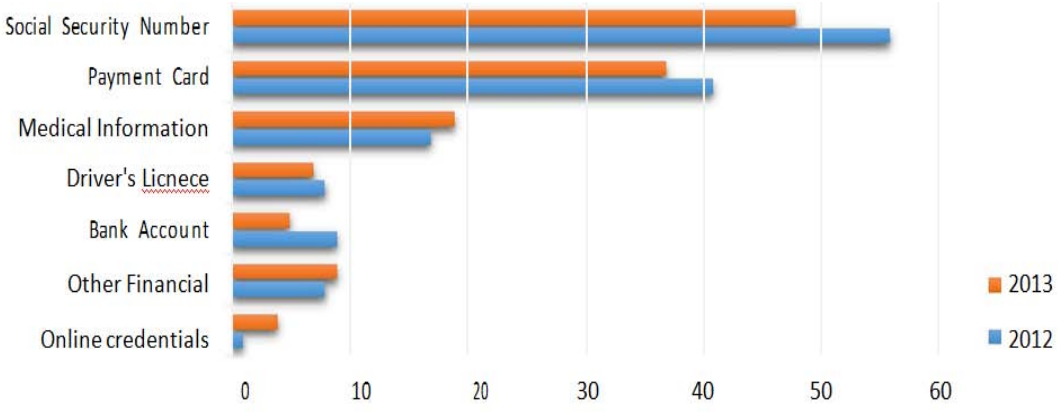


Figure 1 [2]: Percentage of Total Breaches

The bar graph below in Figure 2 illustrates the percent of breaches in 2012 and 2013 in USA, California. While it divided by type of data breached.

Type of data breached



	Online credentials	Other Financial	Bank Account	Driver's Licnece	Medical Information	Payment Card	Social Security Number
2013	4	9	5	7	19	37	48
2012	1	8	9	8	17	41	56

Figure 2 [3]: Total is >100% because some breaches involved more than one data type

From that we can clearly see statistics and some kinds of problems and real problems that can affect any healthcare organization and how the healthcare organizations are the most targeted. So, how can we resolve these problems? What are the solutions?

However we have to search always on solutions that are less cost than the cost of the damage.

There are some of general solutions ideas that can be helpful to reduce the risk of breaches such as:

1) Installing Endpoint security software: By installing endpoint security software we can build up the level of security while on each endpoint security there will be an including of antimalware, antispyware and antivirus. Furthermore there will be some kind of control on devices that employees are using in the healthcare organization that may contain too sensitive data or information such as PHI (Protected Health Information).
2) Limiting the use of personal laptops or mobiles by employees. While all laptops and mobile or any other devices they will use must be affiliated to the healthcare organization.
3) Develop a data recovery: developing a data recovery will help to recover any deleted data. Whereas there are many events recorded in last period about hacked servers and computers while hackers they deleted data and information from it. In instance, one of that events was on February 23, 2012 while one of the hackers could access to one of the computers at a University of Houston (UH) college of Optometry neighbourhood clinic and deleted the records of 7.000 persons.[2]
4) Encrypt all laptops, Mobiles and any devices with strong passwords that contain letters, numbers and symbols to be safe if any one of those devices has been theft or been lost.
5) Protect the Emails Accounts.
6) If there are any need to have Wi-Fi or any kind of network in the healthcare organization is better to separate between guess network and the main network.
7) Train well staffs on all systems used in the organization. It is because without perfect team can use systems and understand well what is going on in any cases, all systems will be weak.

Furthermore, there are many other solutions and methods can be helpful to climb the level of security in organization as creating some kind of algorithm or developing new systems. However this kind of solutions can be very expensive and take much of time, also the result is unknown. Thus, the best thing is to try protecting the organization by systems that already created and tested before.

On the other hand, in this age of information technology sometimes we forget that paper records still exist and using by organizations and still include sensitive information on them. While paper records facing the same problem that facing by technology part. Paper records can be lost, stolen and breaches. More than that there are other problems that are Incorrect Mailing and Improper Disposal that can effect negatively on the security of data.

The two pie charts below Figure 3 and Figure 4 show some statistics of breaches and breached records by type in USA.

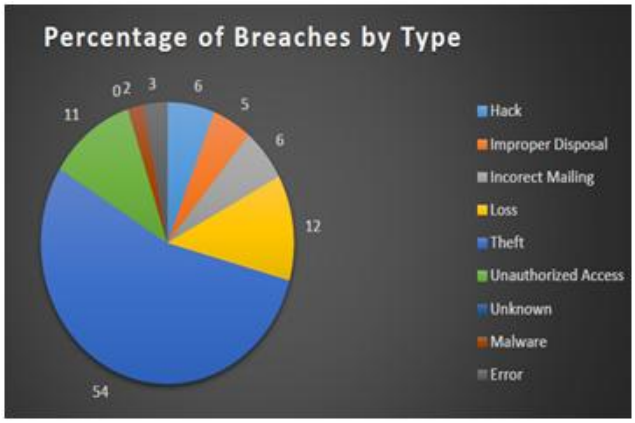


Figure 3 [4]: Percentage of Breaches by Type

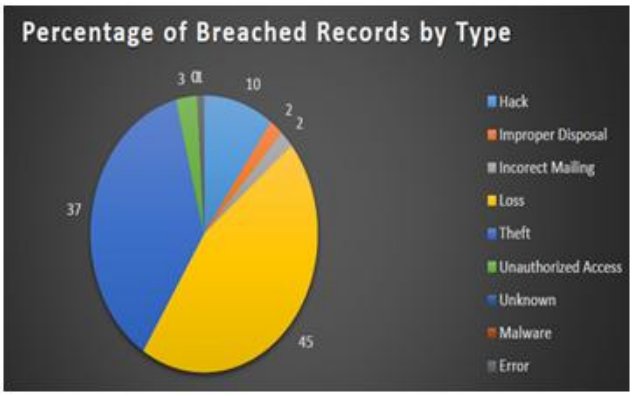
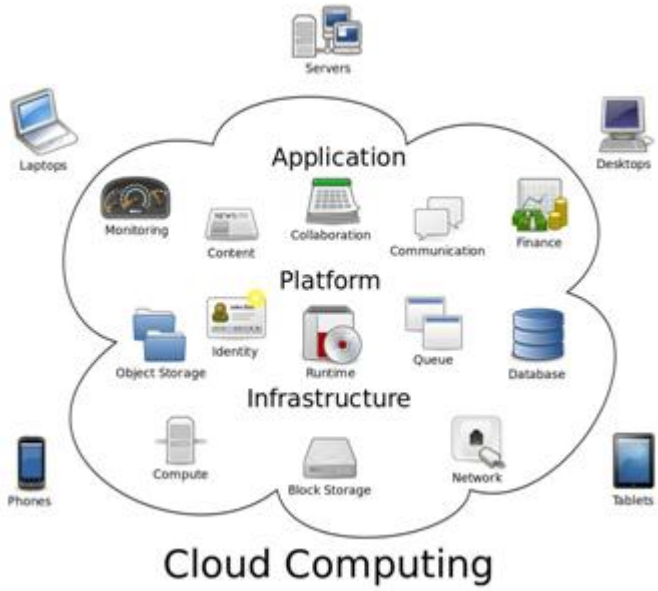


Figure 4 [4]: Percentage of Breached Records by type

3. Healthcare and Cloud Computing

Cloud computing is a group of integrated and connecting hardware and software using the internet for communication and transport provides hardware, software and networking services to clients. In light of security problems that faced by healthcare organizations while the protection of individuals' information is the major concern facing the healthcare organizations. [5] [6



Is it possible to mitigate the risk of breaches by using cloud computing? If the answer is yes, so how?

Using cloud computing in healthcare organizations will not eliminate the risk of breaches. It will just reduce the risk.

In fact if we take the last statistics Figure 3 as an example we can clearly see that Cloud computing can be one of solution that can increase the level of security in the organization.

However, it does not mean that cloud computing is full secure, while there are many kind of methods and strategies that can help in increasing the level of security in any healthcare industry, while those techniques still in the field of cloud computing, such as developing a cloud platform, whereas a cloud platform must first be established, to allow each hospital to apply for its own cloud server without having to do its own setup, and to allow the hospital to manage and save its electronic medical record information. In addition, the electronic medical records of each hospital may be exchanged and shared through this platform. Medical personnel can log into the cloud platform and upload the generated electronic medical records. The established cloud platform can not only be used by hospitals, but patients may also log into the health care cloud to search for their own medical record information. In the mechanism provided, the communication between each role is presumed to be via a secure transmission channel, such as the SSL/TLS (SSL and TLS, to ensure data exchange security [7]. Whereas TLS (Transport Layer Security) and its predecessor is SSL (Secure Sockets Layer) both of them present a cryptographic method (SSL) developed to increase the communication security between any two devices [8].

	Using Intern Hardware and System	*Using Cloud Computing*
Theft	YES	NO
Loss	YES	NO
Unauthorized access	YES	YES
Hack	YES	YES

4. Conclusion

All in all, Healthcare organizations is one of most sectors facing the risk of breaches in many countries especially in USA. While this weakness is due to many problems in the security system and in the preparing of staffs who are working in this sector who are in turn responsible to protect all information from any kind of breaches whether electronic breaches or physical breaches (physical records).

Therefore should be there kinds of solutions or ideas to fix that problems and eliminate the weakness to climb the level of security and privacy and to protect individuals' information considering the cost of that solutions. Some of those solutions are:

1) Installing Endpoint security software.
2) Limiting the use of personal laptops or mobiles by employees.
3) Develop a data recovery.
4) Encrypt all laptops, Mobiles and any devices with strong passwords.
5) Protect the Emails Accounts.
6) Separate between guess's network and the main network.
7) Train well staffs on all systems used in the organization.
8) Using Cloud Computing. However it can be expensive for using.

References

[1] Media Video http://youtu.be/VDrWbjgM3Ik
[2] Chris Hourihan and Bryan Cline, A Look Back: U.S. Healthcare Data Breach Trends, December 2012.
[3] Kamala D. Harris, California Data Breach Report.2014
[4] Chris Hourihan and Bryan Cline, A Look Back: U.S. Healthcare Data Breach Trends, December 2012.
[5] The Notorious Nine, Cloud Computing Top Threats in

2013, Cloud Security Alliance.2013
[6] Trevor Strome, Must-knows about cloud computing in healthcare .2014.
[7] Zhuo-Rong Li, En-Chi Chang, Kuo-Hsuan Huang, Feipei Lai. A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform, 2013
[8] SANS Institute InfoSec Reading Room, SSL and TLS: A Beginners Guide, 2003.

Author Profile

Ahmed Mohamed Mahmoud, Faculty of Information and Communication Technology, IIUM, Kuala Lumpur, Malaysia.

Akram M Zeki, Faculty of Information and Communication Technology, IIUM, Kuala Lumpur, Malaysia.