Data Breaches in Healthcare: A Case Study

– **Avisha Rathee**
Bachelor of Computer Applications (BCA) 4th Semester, Amity University Noida, India
https://orcid.org/0000-0001-7857-8046 avisharathee05@gmail.com

As cyber crime continues to grow around the industries, medical identity theft and even the medical data breaches are vividly rising at disproportionate rates. Although all identity theft can greatly result in catastrophic damage to the customer's financial wellbeing the medical identity theft can even affect the physical health of the customer. Nowhere even the impact of Cybercrime has greatly reached to extreme levels and is proving very disastrous even in the healthcare fields. In just the first few months of 2014 there were 51 healthcare/medical data breaches cases that arrived, according to the identity theft resource centre. In this I am even going to discuss one of the famous water breaching cases that occurred in Queensland, Australia which is famous for 2,000 MAROOCHY water attacks. This paper will show the mistakes of the workers in system handling. The lesson learned from this incident proved very helpful in the establishment of new agendas both in SCADA security system and Medical science.

Keywords

- Data Breaching
- Healthcare System
- Data Security
- Data Handling Cyber-Attack

ARTICLE HISTORY
Paper Nomenclature: Case Study (CS)
Paper Code: CYBNMV2N2FEB2020CS1
Submission Online: 07-Feb -2020
Manuscript Acknowledged: 08-Feb-2020
Originality Check: 10-Feb-2020
Originality Test Ratio: 4% (Turnitin)
Peer Reviewers Comment: 15-Feb-2020
Blind Reviewers Remarks: 17-Feb-2020
Author Revert: 19-Feb-2020
Camera-Ready-Copy: 25-Feb-2020
Editorial Board Citation: 29-Feb-2020
Published Online First: 13-May-2020

Data Breaching In Medical Field

The Identity Theft Resource Centre (ITRC) Breach Reported Hits Record In 2014.

There are more than 5000 breaching cases and 675 million records exposed after 2005.

According to a recent report released by the ITRC on 12 January 2015, the number of O.S cases of data breaching tracked hit a record of 783 cases in 2014 sponsored by IDT911. In 2010 there were 662 breaches tracked and now since 2005 a milestone of 5,029 data breach incidents have been reported which involves more than 675 million estimated records.

There were various types of breaches followed in the year (2007-2016) that included INSIDER theft, hacking, data on move, accidental exposure, subcontractor/third party, employee negligence.

The ITRC Breach List

The ITRC breach list is the complete list of data breaches which was confirmed by the various media sources and the list from state Governmental agencies. Breaches potentially led to the identity theft, which even included social security numbers, driver's license number, the financial account information and medical information.

Some of the Recent Healthcare Data Breaches on National and International Basis.

1. Healthsource of Ohio on March 17, in Minford announced the personal, financial and health information of around 8,800 patients who compromised when the health system of the hospital put the patient information into a software web program that was not at all password protected.
2. On March 4, S.C-based Roper hospital, Charleston, announced that the faxes that contained Patients healthcare information has been sent to a man in Portland, Ore.
3. The Pittsburgh-based UPMC announced that on March 6, the data breach has compromised all the personal information of the 322 UPMC employees.
4. On March 13, the DMC (Detroit Medical Centre) Harper University

Hospital notified that around 1,087 patient documents with their personal health information were found with one of the hospital employees during an Identity Theft Investigation.

5. On March 14, Glenwood, Colo-based Valley View Hospital announced that they have suffered data breaching when the hackers introduced the virus into the computer system of hospital that took Screenshots of around 500 patient personal records.

6. On March 12, the UCSF were notified that 9,986 of their patient information which was stored in the computers were stolen from the UCSF family medicine centre.

7. On March 6, medical facilities Los Angeles County announced that 168,500 patient data which was contained on computer equipment was stolen from the contractor's office.

8. On March 10, at Atlanta based Emory Healthcare had announced that an employee laptop that contained personal information of around 826 patients had been stolen from a vehicle at one of their clinics.

   a. The Calif based St. Joseph Healthcare at Irvine announced on March 12, that mistakenly they have released protected health information of 11,800 patients.

High point, N.C-based, March 11, Cornerstone Healthcare announced that they have altered more than 500 reports which contained patient personal information that was stolen from Cornerstone Neurology, a practice location for doctors. [Ref 1]

The Trends in the Healthcare Data Breaching

As the healthcare regulation like HIPPA have become more in trend or pervasive, and the healthcare reports have been moved online, the healthcare field has come greatly into the target of hackers and fraudsters and they are even becoming more and more vulnerable to breach by accidents (such as stolen/lost laptops).

According to the Red spin 2011 the PHI breach analysis report showed that almost 19 million patients suffered from health records and almost 59% of all breaches involved business associates.

The rise of Healthcare data breaching has vividly increased day by day. Last year, the Second Annual Survey of PONEMON INSTITUTE on medical identity theft gave that more than 1.49 million Americans were targeted by this crime.

Some of the Basic Points that was taken away from Red Spin Report are-:

1. The Federal government should update the Accountability Act and the Health Insurance Portability Act of 1996 (HIPPA) Security rule so that the healthcare providers have more practical guidance.
2. Healthcare providers should make their employees more security concerns.
3. Healthcare providers should always conduct HIPPA risk analysis on bi-annual basis and action should be taken against any vulnerability found.
4. Hospitals should conduct portfolios risk analysis of the contractor, numerous vendors, and the consultants the work which focus on the present high risk from data breaches. [Ref 7]

Five ways to Avoid the Healthcare Data Breaching in Medical Science

1. Always conduct an annual HIPPA security risk analysis.
2. Always inoculate yourself by encrypting the data-at-rest.
3. Conduct for the more frequent vulnerability assessment and the penetration testing.
4. Try to invest in the security awareness of your following workforce.
5. Always try to engage with your following business associates.

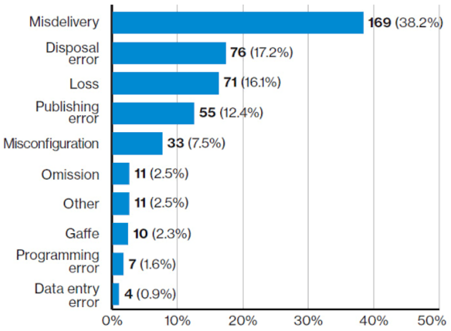


Figure 3. Top threat action varieties within Error, n=442

Maroochy Water Breach, Queensland, Australia

Maroochy Shire Sewage System

1. SCADA controlled system which had 142 pumping stations over an area of 1157 square km was installed in 1999.
2. In this SCADA controlled system there took a water breaching attack which was a kind of revenge taken by one of the dismissed employees of the system.
3. In 2000, the area sewage system was having 47 unexpected faults cases causing extensive sewage spillage over an area.

Scada Control Sewage System

1. Special purpose controlled computer was set up at each station to control the valves and alarms of the entire system present in that area.

Volume - 2
Issue - 2
February
2020
e-ISSN
2582-5755

2. Each system was having communication with and was controlled widely by the central control centre.

3. Communication that occurred between the pumping station and the control centre was with the help of radio, rather than wired networks.

What Happened Basically In Queensland?

1. More than 1 million litres of the untreated sewage wastes was released into the waterways and the local parks polluting the entire environmental system.

Technical Problems that Occurred.

1. The sewage pumps of the entire system did not operate when they should have been operated.

2. Alarms that was set-up in the entire system did failed out to report the problem to control centre

3. Last but not the least there were a lot of communication issues between the control centre and the pumping stations.

Insider Was The Main Cause….

1. VITEK BODEN who worked for hunter Water tech (he was the system supplier) was having the entire responsibility for the MAROOCHY system installation. He had some disagreements with the company so he left in 1999.

2. After leaving the company he tried to get a job with the local councils but was refused and then he decided to take revenge against the system.

Revenge By Boden

1. Boden was very angry and then he decided to launch attacks on the entire SCADA control systems.

2. He hoped that the HUNTER WATER TECH would only be blamed for the system failure.

3. This was basically an insider breach attack in which the insider do not have to work in the organisation and even can cause harmful imbalance to the system by breaching the data of the system.

How It Happened?

1. VITEK BODEN was successful in stealing a SCADA configuration program from his working employers and when he was leaving the organisation, he installed the program in his own laptop.

2. He even stole radio equipment and a control computer that was set-up and which could be impersonating the entire genuine machine at each of the pumping stations.

3. Whereas, insecure radio links were being used to communicate with pumping stations and then lastly their configuration were changed.

Incident Reports

1. After all the analysis of communication it was concluded that it was caused by the deliberate interventions that occurred in the system and it always occurred by the specific station.

2. Actions were taken as the entire system was configured so that ID was not used as the messages from ID station were malicious.

3. BODEN'S car was captured and the stolen computer system was discovered. He was put under surveillance.

Causes Of The Entire Problem

1. There was a lack of monitoring and logging.

2. None of the staff was well trained so that he/she can recognise the Cyber attack.

3. Installed system was completely insecure.

4. The radio links were very insecure for system communication.

Final Punishment

On October 31, 2001 VITEK Boden Was Found Guilty Of:

1.26 counts of wilfully using the computer system to cause severe damage.

2.1 count of causing very serious environmental harm.

He was jailed for two years.

Lesson Learned

After analysing all the problems STRINGFELLOW said that the problem is not with the system installation but it is a cyber attack due to which none of the system is working properly. With the help of advanced tools, he got to know the real cause and finally secured the SCADA system. Lots of lessons were learned from this incident. They are:

A) It was very difficult to protect against insider attacks.

B) The radio system was a very insecure method of communication.

C) SCADA devices should be secured both physically and logically.

D) System should contain all the previous records which involve control and connection from remote sites.

E) Using passwords and firewalls along with encryption can keep the entire system safe.

F) A proper set of trained members should be allotted to the system so that he/she can get acknowledged if it is a cyber attack and even always update the system software. [Ref 2]

Methodology

I have chosen the advanced methods to describe the topic of my term paper that is data breaching in the medical field and mariachi water attack, Queensland, and Australia. I have referred to articles and several internet sites for this project. I have even discussed the matter at international level showing various cases of data breaching in medical science (HIPAA) and how it leads to financial crisis as well as healthcare issues. Maroochy water attack (SCADA) was the great exam of data breaching in the technology world.

Conclusion

Well, I can conclude that the ubiquity of the SCADA system in information technology industry and HIPPA system in medical field and the inherent vulnerabilities, the legacy components and the proprietary hardware and software gave entire exposure to the external attack on the systems.

After the external attack on MAROOCHY WATER SYSTEM no one could analyse that it was an external attack even though everyone was blaming the installation process of the system, software was blamed because of the untrained members working in the system.

Similarly, when the external attack was started on insecure network sites of HIPPA, medical field there were lots of financial as well as healthcare issues to the customers/patients.

This is just prime examples about the kind of attack that can be done on the systems of any of the working fields. Now the entire department should be ready to face challenges because the attack can even grow further and give rise to devastating terrorist attacks.

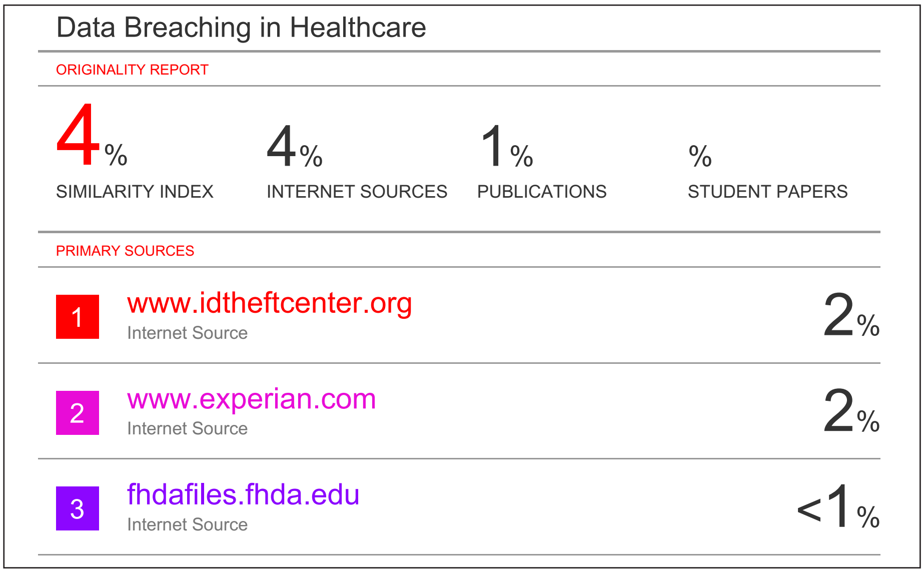
Avisha Rathee is a student of Amity University, pursuing her bachelor's degree in computer science, (B.C.A). She has always been highly interested in computer science technology & programming. . She is learning many computer languages like python; Php etc to have a bright future in the IT field .She is currently looking forward to examining Cyber Security as her leading career along with the fundamental knowledge of software development.

.

avisharathee05@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
10-Feb-2020	Turn-it-in	~~2158~~	~~11804~~



Data Breaching in Healthcare

ORIGINALITY REPORT

4%	4%	1%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.idtheftcenter.org Internet Source	2%
2	www.experian.com Internet Source	2%
3	fhdafiles.fhda.edu Internet Source	<1%

Note: The Cybernomics had used the urkund plagiarism [http://www.urkund.com] tool to check the originality.

Reviewers Comment

Review 1: As of now… The number of reported healthcare data breaches has been steadily increasing each year. Except for 2015, the number of reported healthcare data breaches has augmented every year.

Review 2: According to the 2018 Verizon Data Breach Investigations Report (DBIR), the past year alone saw 536 healthcare breaches.

Review 3: The new smart card badging solution significantly lowered the risk of data breaches while creating a simplified user experience. Login via a smart card combined with an eight-digit numeric PIN is easy to use and eliminates the frustration of frequent password changes.

Editorial Excerpt

The article has 4% plagiarism which is accepted percentage for publication. The investigation determined patient demographic details, medical claims data, and other personal information were potentially breached. But when Immediate sent the notifications to patients about the security incident, some patients reported that they were receiving multiple letters, some addressed to other patients. Michigan Attorney General is investigating the incident. After Editorial board decision under the group of Case Study.

Acknowledgement

Author is highly indebted to Scholastic Seed Inc & amp; editorial team of Cybernomics, For making the write-up in the shape of an article.

Disclaimer

All views expressed in this paper are my/our own. Some of the content is taken from open source websites & some are copyright free for the purpose of disseminating knowledge. Those some We/I had mentioned above in the references section and acknowledged/cited as when and where required. The author/s has cited their joint own work mostly, Tables/Data from other referenced sources in this particular paper with the narrative & endorsement has been presented within quotes and reference at the bottom of the article accordingly & appropriately. Finally some of the contents which are taken or overlapped from open source websites for the knowledge purpose. Those some of i/we had mentioned above in the references section.

Citation

Avisha Rathee
“Data Breaching In Healthcare:-
A Case Study”
Volume-2, Issue-2, Feb 2020.
(www.cybernomics.in)

Frequency: Monthly, Published: 2020
Conflict of Interest: Author of a Paper
had no conflict neither
financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in
https://orcid.org/0000-0002-7952-096X