Data Breach Risk Factors in the Healthcare Industry

Nick Barilovich

IAAS 795 Capstone

Davenport University

Dr. Lonnie Decker

11/10/16
Table of Contents

Chapter 1 - Introduction................................................................................................... 3
Chapter 2 – Literature Review......................................................................................... 5
Chapter 3 – Research Method .......................................................................................... 13
Chapter 4 - Results ....................................................................................................... 15
Chapter 5 – Conclusions and Suggestions for Further Research ................................. 17
Works Cited................................................................................................................... 21
Appendices ................................................................................................................... 23
Chapter 1 Introduction

Within the information security industry, it is commonly known that the healthcare industry is subject to heavy attack by hackers attempting to access valuable personal and health information. In fact, HealthDataManagement.com reports that personal health information is up to fifty times more valuable than plain personal information (HealthDataManagement.com). On a whole, data breaches have been steadily increasing in number and severity over the last ten years (Denale and Weidenhamer, 2016). Data breaches should be a growing concern for any company or organization that conducts business on a computer that is connected to the Internet. According to the U.S. Census Bureau, more and more business is being conducted online. Online shopping is not the only focus of data breaches. Companies such as Target store its customers’ proprietary credit card information on its own servers. That presents a great target for hackers.

Individuals and families are also at risk of having personal information stolen from home computer networks. Access may be unknowingly achieved through unsecured routers or through a phishing attack. Hackers profit from stealing personal information for use themselves or for sale to other people. In the right, albeit nefarious, hands, personal information is extremely valuable. Pilfered personal information may not only be used to steal that person’s identity to open credit cards and mortgage real property, but also to create false documents for use in the healthcare industry and commit insurance or Medicaid fraud.

Certain companies or organizations may be more at risk than others when it comes to data breaches. There are certain risk factors that make companies or organizations
more prone to being a victim of a data breach. The healthcare industry, in general, is more at risk than other industries. Some risk factors are more significant to the healthcare industry. Among those risk factors are: 1) lack of information security awareness training programs for non-IT employees, 2) lax access control for server rooms, 3) lack of password standards, 4) lack of data back-up systems and, 5) meager IT/InfoSec budgets.

For any company or organization that either possesses valuable information, conducts business on the Internet, or is connected to the Internet, data breaches are a growing concern. Within the last five years, there has been a large push in the healthcare industry to move away from traditional paper records and into electronic document management. The more valuable the possessed information is perceived to be, the more at risk for a data breach the company or organization is. Hackers are attracted to companies or organizations with certain characteristics. Identifying risk factors associated with data breaches will help companies and organizations to mitigate risk and prevent future data breaches. Recognizing and facing risk factors will also serve to protect those companies most at risk for a data breach.

Some of the research questions addressed in this thesis paper are:

1. What are the common risk factors among healthcare organizations that have been the victims of data breaches?
2. What can be done to mitigate the identified risk factors?
3. What are some common characteristics of those healthcare organizations which have not experienced a data breach?
4. How do victimized healthcare organizations react to data breaches and what
common protections do healthcare organizations add to prevent future incidents?

5. How do healthcare organizations mitigate the damages to patients/consumers and
how satisfactory is the mitigation?

6. What steps should healthcare organizations take to ensure that the organization is
not re-victimized by a second or third data breach?

Another issue that will be examined in my research are the things that healthcare
companies or organizations are doing to ensure that they do not become revictimized
by a second or third data breach.

Data breaches are currently a phenomena without definitive cures. Many
healthcare companies and organizations have no warning when an incoming data
breach is occurring, and are left trying to pick up the pieces after an attack. Healthcare
organizations are rightly responsible for the integrity of the data collected on their
servers. After a breach, not only is the post-breach clean-up expensive for the
organization and the consumer in the form of credit monitoring, but the loss of trust may
be more damaging than the monetary damages.

**Chapter 2 Literature Review**

One of the main reasons that data breaches are getting so much attention in the
media is because of the amount of money that data breaches cost American
corporations and consumers. Some consumers whose personal information has been
accessed as a result of data breaches have joined to initiate class action lawsuits in an
effort to recoup some of the financial losses incurred. The plaintiffs allege some sort of
loss, which is usually monetary and that the company or organization that they
Data Breach Risk Factors

entrusted with their personal information was somehow negligent in dealing with their personal information. In his article entitled “Data Breach Class Actions,” Richie confirms that these class action lawsuits have been successful. The author states in his conclusion that with data breaches becoming more common and costly, class action lawsuits may be an option for consumers to put corporations in check and hold them responsible for information security (Richie, 2015).

Healthcare companies are the target of many data breaches because of the type of information that they possess. Kamoun and Nicho wrote an article about the dangers and risk factors of data breaches in the healthcare information business sector. The authors acknowledge that the transition from paper records to electronic document storage demands the highest security. Kamoun and Nicho state that data breaches are especially troublesome in the healthcare field because medical information is some of the most personal information there is. Unfortunately, innovations in the security systems in healthcare organizations have not kept pace with technology. The authors identify many different end point users that are especially weak points for a data breach. Some of those points are: ambulatory healthcare providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, health maintenance organizations, and outsourced service providers (Kamoun and Nicho, 2014).

According to the authors, because healthcare organizations are responsible for the client/patient personal information, the organization suffers when that information is disclosed, regardless of the intent of the disclosure. The healthcare organization may lose clients as a result of negative publicity and may even have to pay damages to the clients. There are many legal and ethical considerations that healthcare companies
must consider when dealing with their clients’ personal information. Healthcare companies have a legal and ethical duty to protect their customers’ personal information to the best of their ability (Kamoun and Nicho, 2014).

The Ponemon Institute is a research institute that is based in Traverse City, MI. Every year for the past ten years, the Ponemon Institute has compiled a study about the frequency and cost of data breaches for companies and organizations across the world. Cyber-attack data is typically categorized as those attacks occurring domestically in the United States and those occurring outside of the U.S. Study results reveal that since the Ponemon study was initiated, the cost of a cyber-attack or data breach has been constantly and steadily increasing.

There are many costs associated with a successful data breach. According to the Ponemon Institute’s study, the highest costs are those associated with lost customer business, legal defense services and investigations and forensics. The average cost of a single successful data breach for an American company is $6.5 million (Ponemon Institute, 2015). This figure does not take into account the cost of the pre-existing cyber defenses which may have already been in place before the cyber-attack defenses were in place.

Certain industries are more susceptible to data breaches. The three industries identified as most at risk are financial, healthcare and technology. Cyber criminals and criminals in general are usually pursuing the most lucrative monetary gain. It makes sense that these industries would be targeted the most, since they have access to the most personal information. The study does demonstrate that there is a need to be
concerned about data breaches both now and in the future. The Ponemon study merely provides the cost data for data breaches. It does not make any recommendations on what can be done to reduce the occurrence of data breaches or reduce the cost of data breaches for organizations. The Ponemon Institute provides a rich source for investigative research on the issue of cyber-crime and the healthcare industry. It can be inferred from the results of this study that something needs to be done in order to curb the expansion of cyber-crime (Ponemon Institute, 2015).

The Ponemon Institute’s study is the primary inspiration for my thesis project. I plan to analyze and make recommendations based upon some of the findings in the Ponemon Institute study. The Ponemon study provides data on all aspects of data breaches, including, number of records accessed, company training programs, software update programs, the field of the company that fell victim to a data breach, the feelings of the company’s employees and many others factors. Participants in the study are from American companies in many different fields. However, the largest population comes from the healthcare industry (Ponemon Institute, 2015).

Here are the key findings from the Ponemon Institute’s study:

• “80 percent of all surveyed organizations are concerned about the consequences of a large public data breach;

• 17 percent of respondents have experienced a data breach that they are aware of over the previous 12 months;

• The vast majority of the data breaches experienced are small consisting of a loss of fewer than 500 records;

• The median data breach is 100 records;
• Only 45 percent of respondents believe their company has adequate resources to detect all breaches;
• 75 percent of respondents have developed an incident response plan but only 42 percent have tested the plan;
• 60 percent of respondents said that the information technology (IT) department is responsible for managing the data breach response;
• 64 percent purchase cyber insurance;
• The vast majority of breaches fall below the cyber insurance policy deductible;
• Most organizations use internal resources to manage small breaches;
• 51 percent have selected data breach response vendors;
• 75 percent prefer to receive all cybersecurity risk services from a single vendor” (Ponemon Institute, 2015).

David Khey and Vincenzo Sainato wrote an article entitled “Examining the correlations and spatial distribution of organizational data breaches in the United States.” The authors acknowledge that there is a lot of data available about data breaches, but there has not been much analysis of the data. The authors of this article talk about the risk profiles of companies who have been a victim of data breaches. These risk profiles are created by examining companies or organizations that have fallen victim to data breaches. The companies are categorized based on their characteristics. The authors hope to determine which company characteristics are most indicative of a company likely to be a victim of a data breach (Khey and Sainato, 2013).
The authors report that not all companies report data breaches in the same manner. Privately held companies technically do not have to disclose information about data breaches that have occurred on their servers. Data for this study was collected through the Privacy Rights Clearinghouse. The goal of the authors was to identify the most common risk factors amongst companies who have been victim of a data breach so that other companies will be able to prevent data breaches and mitigate risk in the future (Khey and Sainato, 2013).

Khey and Sainato were unable to find any “discernable pattern of victimization of particular industries or breaches within specific geographies or timeframes” (Khey and Sainato, 2013). One other idea that the authors identified through their analysis is that states with harsh penalties for perpetrators of data breaches do not have a lower occurrence of data breaches. Interestingly, the authors found that jurisdictions within the United States with harsher penalties for those found guilty of cyber-crimes did not have a lower incidence of data breaches. Khey and Sainato mentioned New York and California as two states that have harsh penalties for perpetrators of data breaches. Khey and Sainato advocate that organizations or companies that want to limit their exposure to data breaches should maintain a multi-layered approach to their information security. There should be more than one system in place to protect stored information within the company. Finally, the authors state that companies should be fully responsible for their own information security and that they should also take it extremely seriously (Khey and Sainato, 2013).

Adam Foresman wrote an article entitled “Once More Unto the (Corporate Data) Breach, Dear Friends” that identifies the need for legislation on data breaches. The
author states that current data breach reporting and repercussions for companies who have been victim of a data breach are insufficient. Foresman begins his article by stating that the Private Securities Litigation Reform Act (herein after referred to as PSLRA), a law which governs how privately held companies respond to class action litigation (15 U.S. Code § 78u–4), was created to give direction on protecting the information contained in trading securities. The author states that PSLRA receives failing grades when enforcing information security. It is not strong enough (15 U.S. Code § 78u–4).

Foresman believes that the government should create regulations to monitor and punish companies who have been the victim of a data breach and have failed to employ appropriate information security standards. The general consensus between information security professionals is that most data breaches occur because of employee negligence or human error. Individual general employees do not consider the sensitive nature of information security to be of importance (Foresman, 2015).

In a paper published by Cleardata, the company recounts three highly publicized data breaches in the healthcare sector as case studies. The data breaches highlighted in the case studies occurred at Community Health Systems, Advocate Medical Group and Cogent Health in 2013 and 2014.

In the Community Health Systems data breach 4.5 million patient records were accessed by a hacker who uploaded malware to the company’s electronic documents system and transferred the data outside of the company servers. Community Health
Systems implemented encryption protocols, intrusion detection measures and some rules and regulations for regular employees (Cleardata).

In the Advocate Medical Group data breach, hackers targeted unencrypted end user laptops to access another 4.5 million personal health records. The laptops were stolen and their passwords were cracked. After the data breach Advocate Medical Group hired 24/7 information security monitoring personnel and implemented technically advanced information security safeguards. Advocate Medical Group acknowledged that the personal health information should not have been loaded onto laptops that were not encrypted (Cleardata).

Cogent Health’s data breach was a result of carelessness by a third party transcription service. The transcription company stored Cogent Health’s clients’ personal health information on a Google server that was not secured. 32,000 client records were accessed. Cogent severed ties with the transcription company and obtained the hardware that the patient information was stored on from the transcription company (Cleardata).

From March to October 2012, Carolinas Medical Center did not know that they were the victim of a data breach. The breach occurred through a provider’s email server. Neither the medical center nor the provider knew that confidential emails were being intercepted by a third party. About 5,600 patients’ personal health information was accessed, including social security numbers, diagnoses, names, birth dates and hospital visit data (Walsh, 2012). The data breach was only discovered after a software update. After the Carolinas Medical Center discovered the data breach, the hospital
notified law enforcement and upgraded their information security hardware and software to include intrusion detection and active monitoring. Those types of systems were not employed by the Carolinas Medical Center prior to the data breach (Walsh, 2012).

Chapter 3 Research Method

The research method used in this thesis paper is meta-analysis. Data from secondary sources shall be combined with analysis to make conclusions and recommendations based upon the data. The analysis of four to five case studies would be optimal for the best sample. Data about the breaches occurring in healthcare organizations shall be gleaned from scholarly articles and popular news sources. Both qualitative and quantitative data are necessary to formulate this thesis. I can pick and choose elements from either type of research to formulate my thesis data.

The steps in conducting meta-analysis are:

1. Problem Formulation – The problem is that certain companies are more at risk than others when it comes to data breaches. Each company has different risk factors. Determining which risk factors are most indicative of risk would be critical to determining how to mitigate that risk.

2. Searching Databases – Databases on the Davenport University website, Proquest and Academic OneFile will be accessed and employed in this thesis.

3. Criteria for Review – The studies in this thesis will be coded for comparison of the samples.

4. Effect Sizes – In this step, the statistical analysis of the data is completed.
5. Summary Effect – Summary effect will be employed. The summary effect allows the researcher to compare subgroups from different studies, even though they may have had different sample characteristics.

6. Interpretation – The results of the summary effect will be interpreted to reveal correlations and differences between the study samples (Creswell, 2011).

The study population includes American companies or organizations who have been a victim of data breaches from the beginning of 2010 to the present. The term “organizations” includes some non-profit healthcare organizations which have been the victim of a data breach. There may be significant similarities between these non-profits and healthcare organizations.

Table 1:

<table>
<thead>
<tr>
<th>Healthcare Organization</th>
<th>Start Date</th>
<th>End Date</th>
<th># of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Health System</td>
<td>08/01/2014</td>
<td>08/31/2014</td>
<td>4,500,000</td>
</tr>
<tr>
<td>Advocate Medical Group</td>
<td>07/01/2013</td>
<td>07/31/2013</td>
<td>4,500,000</td>
</tr>
<tr>
<td>Cogent Health</td>
<td>06/21/2013</td>
<td>08/21/2013</td>
<td>32,000</td>
</tr>
<tr>
<td>Carolinas Medical Center</td>
<td>03/11/2012</td>
<td>10/08/2012</td>
<td>5,600</td>
</tr>
</tbody>
</table>

Table 2:

<table>
<thead>
<tr>
<th>Healthcare Organization</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Health System</td>
<td>Heartbleed Bug, unprotected test server mistakenly connected to the Internet</td>
</tr>
<tr>
<td>Advocate Medical Group</td>
<td>Stolen laptops that contained unencrypted PHI</td>
</tr>
<tr>
<td>Cogent Health</td>
<td>Transcription service uploaded PHI to an unsecured Google server</td>
</tr>
<tr>
<td>Carolinas Medical Center</td>
<td>Undetected email interception</td>
</tr>
</tbody>
</table>
Table 3:

<table>
<thead>
<tr>
<th>Healthcare Organization</th>
<th>How Discovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Health System</td>
<td>Recognized that the server was connected to the Internet</td>
</tr>
<tr>
<td>Advocate Medical Group</td>
<td>Laptops reported as stolen</td>
</tr>
<tr>
<td>Cogent Health</td>
<td>Information made public and indexed by Google</td>
</tr>
<tr>
<td>Carolinas Medical Center</td>
<td>Operating System upgrade revealed data breach</td>
</tr>
</tbody>
</table>

Table 4:

<table>
<thead>
<tr>
<th>Healthcare Organization</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Health System</td>
<td>Audit and surveillance technology, advanced encryption, more frequent employee password changes</td>
</tr>
<tr>
<td>Advocate Medical Group</td>
<td>Hired InfoSec personnel, employed advanced technical safeguards</td>
</tr>
<tr>
<td>Cogent Health</td>
<td>Severed ties with transcription company and purchased transcription hardware</td>
</tr>
<tr>
<td>Carolinas Medical Center</td>
<td>Intrusion detection hardware/software and active monitoring</td>
</tr>
</tbody>
</table>

Chapter 4 Results

The general themes in the case studies that were examined for this thesis paper are carelessness and negligence. Until recently, healthcare organizations did not value cyber security or information security as much as they should have. In these four case studies alone, over nine million personal health records were accessed without the patients’ knowledge or permission. One issue identified in the case studies was that personal health information was stored, unencrypted, on unsecured servers outside of the organization’s network. Another issue identified in the case studies was that outside vendors did not treat personal information with the same care as the organization (Cogent Health).
The information security chain is only as long as its weakest link. Although Cogent Health and Advocate Medical Group were not directly responsible for the data breaches, they could have done things to prevent them. The main cause of the Advocate Medical Group data breach was employee negligence. Four employees loaded patient personal health information onto their own computers that were only password protected. The information was not encrypted. This should have been a major breach of company policy. This may be an education and awareness issue. It is possible that the responsible parties were not properly educated about the company’s policies and procedures as it relates to removing patients’ personal health information from the protected company servers.

The Carolinas Medical Center data breach was a result of their operating system not being updated when it should have. Companies like Microsoft and Apple monitor current threats and issue patches to their operating systems that are specifically designed to stop attackers from exploiting loopholes or weaknesses. It is not one hundred percent certain that the data breach would not have occurred if the Carolinas Medical Center had updated their operating system’s software, but the chance that the data breach even occurred is lower if the operating system was updated when the patch was originally distributed (Shinder, 2015).

There are some reasons why the Carolinas Medical Center may not have immediately completed the operating system update. Sometimes, IT staff must ensure that their organization’s vital business systems function properly, in a sandbox environment, before distributing the software update to the rest of the network. However, the longer that the IT staff waits, the longer their network may be left
vulnerable. I do not believe that there was any negligence by the Carolinas Medical Center when the operating system update was not installed in a timely manner (Shinder, 2015).

Human error contributed to all four of the data breaches that were in the case studies selected. In the Community Health Systems data breach, at least one employee opened a malicious program that was hidden inside of an email; a data breach ensued. In the Advocate Medical Group data breach, employees left unencrypted personal health information on their computers. The computers were stolen; a data breach ensued. In the Cogent Health data breach, one of the company’s vendor’s employees uploaded Cogent Health’s personal health information to an unsecured server; a data breach ensued. In the Carolinas Medical Center data breach, the healthcare organization’s operating system was not updated in a timely manner resulting in the data breach being discovered much later than it should have. More personal health information was accessed by the attacker because the data breach went undetected for so long.

Chapter 5 Conclusion and Suggestions for Further Research

When conducting research, an inordinate number of data breaches were found in the healthcare industry. It could be concluded that the healthcare industry, as a whole, does not value information security as much as other industries, such as banking, technology or education. However, the recent influx of data breaches and knee jerk legislation has facilitated some change in the way that healthcare companies and organizations employ their information security.
In addition, the healthcare industry has traditionally relied heavily on paper records. In recent years, the industry has quickly converted to electronic document management systems. Research has revealed that healthcare companies and organizations did not upgrade their information security practices, hardware and software in sync with the migration to electronic documents management, leaving the healthcare companies and organizations’ patients’ personal health information vulnerable and under-protected. Healthcare companies and organizations did not have to consider digital information security when they were working with paper documents. Information security no longer means keeping the file room door locked and knowing where the keys are. There may not have been enough budget to upgrade information security systems at the same time as the migration to electronic document management.

In all four data breaches hackers took advantage of weaknesses in healthcare organizations’ information security systems or exploited momentary lapses in security. In the example of the Advocate Medical group data breach, someone was in the right place at the right time and was able to steal the four laptops. Furthermore, they knew the right people to sell the laptops to.

After examining the data breaches at Community Health Systems, Advocate Medical Group, Cogent Health and Carolinas Medical Center, I am able to recommend some changes to healthcare organizations’ information security protocols and practices. The changes are policy and procedure driven and can be implemented with minimal structural or monetary commitment from the company. They are designed to be the most cost efficient solutions to the data breach problems in the health care industry.
The single most significant thing that healthcare companies and organizations can do to reduce the threat of data breaches is to educate their employees about the methods and dangers that hackers pose to their organization. Human error contributed to all four of the data breaches in the case studies that I selected. Any employee that comes into contact with personal health information should be required to complete information security awareness training. This training should include education as to the company’s disaster plan, reporting policies and how to handle personal health information. Consequences for non-compliance with the company’s information security policies should also be included in the training. It is not going to matter how much a healthcare organization spends on information security until its employees are properly trained on how to safeguard their patients’ personal health information.

The commonality between all four of the data breaches included in the case study was the presence of human error. An employee of the company being careless with personal health information resulted in the data breaches at Community Health Services and Advocate Medical Group. In the case of Cogent Health, a third party was responsible for the personal health information being uploaded to an unsecured server. However, Cogent Health was negligent in verifying that their transcription vendor treated personal health information with the same level of care that they do. In the case of the Carolinas Medical Center, IT staff failed to discover that a Heartbleed bug was intercepting emails between a healthcare provider and the medical center. The breach was only discovered and rectified after a system update. It is of utmost importance that all vendors are on the same page with their information security practices. One way to verify this without much effort or hours spent is to do business with companies or
organizations that possess certifications. Certifications are a great way for businesses to advertise that they employ the same type of information security and that it is safe to do business with them.
Works Cited


Sienko, C. (n.d.). Case Study: Health Insurer Anthem. Retrieved from


Appendices